Ekwan E. Rhow (CA SBN 174604)
erhow@birdmarella.com
Marc E. Masters (CA SBN 208375)
mmasters@birdmarella.com
Christopher J. Lee (CA SBN 322140)
clee@birdmarella.com
BIRD, MARELLA, BOXER, WOLPERT, NESSIM, DROOKS, LINCENBERG & RHOW, P.C.
1875 Century Park East, 23rd Floor
Los Angeles, California 90067-2561
Telephone: (310) 201-2100
Facsimile: (310) 201-2110

Jonathan M. Rotter (CA SBN 234137)
Kara M. Wolke (CA SBN 241521)
Gregory B. Linkh (pro hac vice)
GLANCY PRONGAY & MURRAY, LLP
1925 Century Park East, Suite 2100
Los Angeles, California 90067-2561
Telephone: (310) 201-9150
jrotter@glancylaw.com
kwolke@glancylaw.com
glinkh@glancylaw.com

Kalpana Srinivasan (CA SBN 237460)
Steven Sklaver (CA SBN 237612)
Michael Gervais (CA SBN 330731)
SUSMAN GODFREY L.L.P.
1900 Avenue of the Stars
14th Floor
Los Angeles, CA 90067
Telephone: (310) 789-3100
ksrinivasan@susmangodfrey.com
ssklaver@susmangodfrey.com
mgervais@susmangodfrey.com

Y. Gloria Park (pro hac vice)
SUSMAN GODFREY L.L.P.
1301 Ave. of the Americas
32nd Floor
New York, NY 10019
Telephone: (212) 336-8330
gpark@susmangodfrey.com

Attorneys for Bernadine Griffith, Patricia Shih, Rhonda Irvin, Matthew Rauch, and Jacob Watters

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

BERNADINE GRIFFITH; PATRICIA SHIH; RHONDA IRVIN; MATTHEW RAUCH; JACOB WATTERS, individually and on behalf of all others similarly situated,

Plaintiffs,

vs.

TIKTOK, INC., a corporation; BYTEDANCE, INC., a corporation

Defendants.

CASE NO. 5:23-cv-964

FIRST AMENDED CLASS ACTION COMPLAINT FOR:

(1) Violation of the California Invasion of Privacy Act, Cal. Pen. Code § 630 *et seq.*
(2) Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq.*
(3) Statutory Larceny under Cal. Pen. Code §§ 484, 496
(4) Conversion
(5) Violation of the California Unfair Competition Law, Cal. Bus. & Prof.

Code § 17200 *et seq.*
(6) Invasion of Privacy under Article I, Section 1 of the California Constitution
(7) Intrusion upon Seclusion
(8) Violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq.*
(9) Unjust Enrichment

DEMAND FOR JURY TRIAL

Plaintiffs Bernadine Griffith, Patricia Shih, Rhonda Irvin, Matthew Rauch, and Jacob Watters – individually and on behalf of all others similarly situated, file this First Amended Class Action Complaint against defendants TikTok Inc. and ByteDance Inc. (collectively, "Defendants"), and in support state the following:

I. INTRODUCTION

1. This case is about Defendants' unauthorized interception, collection, storing and use of non-TikTok users' highly personal data whenever the non-TikTok users visit a non-TikTok website with the TikTok SDK installed.[1] Defendants engaged in this conduct even where non-TikTok users employed privacy settings that are meant to block third-party tracking of their web activity. This conduct is Defendants' latest salvo in their ongoing campaign to illicitly harvest an enormous amount of private data on U.S. residents.

2. Since its introduction in 2017 as the international version of the Chinese social video app Douyin, TikTok has taken the United States—and the world—by storm. As of 2022, over 1 billion people worldwide and 100 million people in the United States signed up for the TikTok app to create, view, and share short videos popularized by the platform. The success of the TikTok app has allowed its ultimate

[1] Plaintiffs use the term "TikTok SDK" to refer to the TikTok Pixel, the TikTok Events API, and all similar software developed and marketed by Defendants that track the private data of U.S. residents.

owner, Beijing ByteDance Technology Co. Ltd. ("Beijing ByteDance"), to grow from a small Chinese technology company to a multibillion-dollar international conglomerate.

3. But while Defendants TikTok Inc. and ByteDance Inc. (as well as non-party Beijing ByteDance) may have risen to prominence based on the viral videos of adorable puppies and trendy dance moves shared on the TikTok app, they have also become infamous for something far more sinister: invasive and non-consensual harvesting of private user information. Defendants paid $5.7 million to settle allegations by the federal government that they were stealing private information from children. And Defendants paid a $92 million class action settlement relating to allegations that they illicitly made face geometry scans and took private data from millions of U.S. TikTok app users without consent—making all such data available in China, where companies are obligated by law to assist the Chinese Communist Party with intelligence gathering.[2]

4. It is no exaggeration to say that Defendants and their TikTok app are a clear and present danger to personal privacy. Accordingly, many U.S. residents have elected to abstain from using the TikTok app, including many parents who have also taken up the difficult task of keeping their children off the platform for their own safety. As of the time of this filing, Congress is discussing a bill—that has garnered bipartisan support—that would ban or severely curtail the use of the TikTok app nationwide.[3]

5. Unfortunately, a ban on the TikTok app itself would not solve the problem, because Defendants intercept and collect private data from U.S. residents

[2] https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense (China's National Intelligence Law "repeatedly obliges individuals, organizations, and institutions to assist Public Security and State Security officials in carrying out a wide array of 'intelligence' work")

[3] https://www.nbcnews.com/politics/congress/congress-tiktok-ban-social-media-harms-teens-rcna70998

browsing non-TikTok websites—***including U.S. residents who never even used the TikTok app.*** While U.S. residents browse completely unrelated websites to watch their favorite television show, search for medical information, or purchase a birthday gift for their children, TikTok software owned by Defendants and installed on those websites—the TikTok SDK—secretly intercepts and collects their private data and sends it to Defendants. The TikTok SDK is marketed as an enterprise solution for websites to identify their users and deliver targeted ads. Unknown to visitors of these websites, however, the TikTok SDK intercepts and collects sensitive private data and delivers it to Defendants while performing its advertised function.

6. In sum, the TikTok SDK has become yet another, even more insidious, means through which Defendants steal private data from U.S. residents. The purpose of this lawsuit is to put an end to this practice and compensate those injured to the fullest extent of the law.

II. THE PARTIES

A. The Plaintiffs

7. Plaintiff Bernadine Griffith is, and at all relevant times was, an individual and resident of Riverside County, California.

8. Plaintiff Patricia Shih is, and at all relevant times was, an individual and resident of Orange County, California.

9. Plaintiff Rhonda Irvin is, and at all relevant times was, an individual and resident of Tulare County, California.

10. Plaintiff Matthew Rauch is, and at all relevant times was, an individual and resident of El Paso County, Texas.

11. Plaintiff Jacob Watters is, and at all relevant times was, an individual and resident of Madison County, Illinois.

B. The Defendants

12. Defendant TikTok, Inc. f/k/a Musical.ly, Inc. ("TikTok, Inc.") is, and at all relevant times was, a California corporation with its principal place of business in

Culver City, California. Defendant TikTok, Inc. also maintains offices in Palo Alto, California and Mountain View, California. The name change from Musical.ly, Inc. to TikTok, Inc. occurred in May 2019. Defendant TikTok, Inc. is a wholly owned subsidiary of TikTok, LLC, which in turn is a wholly owned subsidiary of TikTok, Ltd. And TikTok, Ltd. is a wholly owned subsidiary of ByteDance, Ltd., a Cayman Islands corporation which is headquartered in Beijing, China.

13. Defendant ByteDance, Inc. ("ByteDance") is, and at all relevant times was, a Delaware corporation with its principal place of business in Palo Alto, California. Defendant ByteDance, Inc. is also a wholly owned subsidiary of ByteDance, Ltd.

C. Alter Ego and Single Enterprise Allegations

14. At all relevant times, Defendants have shared offices in Silicon Valley and also have shared employees. Employees of both companies have performed work on and concerning the TikTok SDK that is at the center of this lawsuit.

15. At all relevant times, and in connection with the matters alleged herein, each Defendant acted as an agent, servant, partner, joint venturer, and/or alter ego of the other Defendant, and acted in the course and scope of such agency, partnership, and relationship and/or in furtherance of such joint venture. Each Defendant acted with the knowledge and consent of the other Defendant and/or directed, authorized, affirmed, consented to, ratified, encouraged, approved, adopted, and/or participated in the acts or transactions of the other Defendant.

16. At all relevant times, and in connection with the matters alleged herein, Defendants were controlled and largely owned by the same person, Beijing ByteDance founder Zhang Yiming, and constitute a single enterprise with a unity of interest. Recognition of the privilege of separate existence under such circumstances would promote injustice.

III. JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§ 1332(d) & 1367 because (i) this is a class action in which the matter in controversy exceeds the sum of $5,000,000, exclusive of interest and costs; (ii) there are 100 or more class members; and (iii) some members of the class are citizens of states different from some Defendants.

18. This Court has personal jurisdiction over Defendants because (i) they are headquartered and/or incorporated in this District, (ii) transact business in this District; (iii) they have substantial aggregate contacts in this District; and (iv) they engaged and are engaging in conduct that has and had a direct, substantial, reasonably foreseeable, and intended effect of causing injury to persons in this District.

19. In accordance with 28 U.S.C. § 1391, venue is proper in this District because (i) a substantial part of the conduct giving rise to the claims occurred in and/or emanated from this District; (ii) Defendants transact business in this District; (iii) one Defendant has its principal place of business in this District; (iv) one Defendant has offices in this District; and (v) two Plaintiffs reside in this District.

IV. GENERAL ALLEGATIONS

A. Defendants' history of misappropriating user data through the TikTok app

20. Beijing ByteDance was founded in 2012 and operates a variety of social networking and news applications, which it regards as "part of an artificial intelligence company powered by algorithms that 'learn' each user's interests and preferences through repeat interaction."[4] As a relative latecomer to the Chinese tech industry, Beijing ByteDance was initially forced to look to overseas markets,

[4] https://www.law360.com/articles/1213180/sens-want-tiktok-investigated-for-national-securitythreats; https://www.cotton.senate.gov/?p=press_release&id=1239

including the United States.[5] Eventually, this view toward international expansion allowed the company to grow at a scale far beyond its peers: as of 2022, Beijing ByteDance had become China's foremost technology conglomerate, valued at approximately $300 billion.[6] Most of Beijing ByteDance's revenue is derived from advertising through its various software and app offerings.[7]

21. Internationally, Beijing ByteDance is most well-known for the TikTok app, a "global phenomenon" with a massive American audience.[8] Starting from a global user base of 55 million in January 2018, TikTok has grown at a staggering rate, passing 1 billion users in September 2021.[9]

22. This meteoric rise has led to a rapid expansion in Defendants' U.S. presence. In 2019, Defendant TikTok, Inc. took over office space in Silicon Valley once occupied by Facebook's WhatsApp messaging app, and began poaching employees from American rivals including Facebook, Snap, Hulu, Apple, YouTube, and Amazon, offering salaries as much as 20% higher.[10]

23. One key to Defendants' financial success was the targeted advertising they ran through the TikTok app, which was made possible through an illicit and highly invasive data harvesting campaign. Through this campaign, Defendants unlawfully accumulated private and personally identifiable information on TikTok users, which Defendants aggregated and monetized to unjustly profit from their unlawful activities.

---

[5] https://www.wsj.com/articles/tiktoks-videos-are-goofy-its-strategy-to-dominate-social-media-isserious-11561780861

[6] https://www.scmp.com/tech/big-tech/article/3193027/tiktok-owner-bytedance-sees-valuation-drop-quarter-us300-billion

[7] https://www.bloomberg.com/news/articles/2019-01-15/bytedance-is-said-to-hit-lower-end-ofsales-goal-amid-slowdown.

[8] https://www.washingtonpost.com/technology/2019/11/05/inside-tiktok-culture-clash-where-us-views-about-censorship-often-were-overridden-by-chinese-bosses/

[9] https://www.cnbc.com/2021/09/27/tiktok-reaches-1-billion-monthly-users.html

[10] https://www.cnbc.com/2019/10/14/tiktok-has-mountain-view-office-near-facebook-poaching-employees.html

24. On February 27, 2019, in response to a complaint filed by the FTC, Defendant TikTok, Inc. (at the time known as Musical.ly Inc.) stipulated to an order mandating a civil penalty in the amount of $5.7 million and injunctive relief concerning their unlawful collection of personal information from children through Musical.ly (the predecessor to the TikTok app)—the largest ever civil penalty of its kind.[11] The subsequent FTC statement indicated that these practices "reflected the company's willingness to pursue growth even at the expense of endangering children."[12]

25. In 2022, Defendants paid $92 million to settle a class action lawsuit alleging that it had been scanning the faces and voices of its users and transferring them to databases controlled by China-based third parties.[13] Immediately after the settlement, Defendants amended their privacy policy to force users to consent to the collection of biometric information.[14] Alessandro Acquisti, a professor of technology policy at Carnegie Mellon University, assessed that this biometric data collection could potentially be put to "chilling" uses against ordinary Americans, including "mass re-identification and surveillance."[15]

26. On August 6, 2020, then-President Donald Trump issued an executive order banning the download and use of the TikTok app within the United States, on the grounds that it "automatically captures vast swaths of information from its users, including Internet and other network activity information such as location data and browsing and search histories" and "threatens to allow the Chinese Communist Party access to Americans' personal and proprietary information — potentially allowing

---

[11] *United States of America v. Musical.ly and Musical.ly, Inc.*, United States District Court, Central District of California, Case No. 2:19-cv-1439

[12] https://www.nbcnews.com/tech/tech-news/tiktok-pay-5-7-million-over-alleged-violation-childprivacy-n977186

[13] https://www.cnbc.com/2022/10/28/tiktok-users-paid-over-privacy-violations-google-snap-could-be-next.html

[14] https://time.com/6071773/tiktok-faceprints-voiceprints-privacy/

[15] *Id.*

China to track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage."[16]

27. While this Executive Order was never enforced, concerns regarding the potential privacy and national security implications of Defendants' U.S. business have only increased. In December of 2022, President Joe Biden signed into law a bill banning the use of the TikTok app on devices used by the federal government's nearly 4 million employees.[17] Media reports also indicate that "momentum is building" within Congress for a complete nationwide ban on the TikTok app.[18] State legislatures have separately been debating a ban on the TikTok app as well, and Montana became the first state to pass a ban in May 2023.[19] Approximately 34 states, as well as New York City, have banned the TikTok app from government devices.[20]

---

[16] https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/

[17] https://www.nbcnews.com/tech/tech-news/tiktok-ban-biden-government-college-state-federal-security-privacy-rcna63724

[18] https://www.nbcnews.com/politics/congress/congress-tiktok-ban-social-media-harms-teens-rcna70998; https://www.nbcnews.com/tech/tech-news/restrict-act-bill-tiktok-rcna73682 (RESTRICT Act); https://www.politico.com/news/2023/10/09/what-happened-to-the-tiktok-ban-00120434 (Guard Act).

[19] https://www.cnn.com/2023/04/14/tech/montana-house-tiktok-ban/index.html; https://www.cnn.com/2023/05/17/tech/montana-governor-tiktok/index.html; https://www.reuters.com/legal/virginia-other-us-states-back-montana-tiktok-ban-court-filing-2023-09-18/.

[20] https://www.wbrc.com/2022/12/14/alabama-gov-kay-ivey-bans-tiktok-state-devices/ (Alabama); https://www.adn.com/politics/2023/01/06/alaska-bans-the-use-of-tiktok-on-state-owned-devices/ (Alaska); https://www.fox10phoenix.com/news/arizona-gov-hobbs-bans-tiktok-on-state-devices (Arizona); https://www.foxnews.com/politics/sarah-huckabee-sanders-bans-tiktok-state-devices-first-move-arkansas-governor (Arkansas); https://www.delawareonline.com/story/news/politics/2023/02/09/delaware-bans-tiktok-on-state-devices/69888579007/ (Delaware); https://apnews.com/article/technology-georgia-8e62e34976ef070a9e24305248981684 (Georgia, New Hampshire);

https://www.eastidahonews.com/2022/12/gov-little-bans-tiktok-on-state-issued-devices/ (Idaho); https://www.wthr.com/article/news/local/indiana-blocks-chinese-owned-app-tiktok-from-state-devices-social-media/531-7bb0ccc2-29b2-47bb-a1be-71aa836b03b3 (Indiana); https://dailyiowan.com/2022/12/14/governor-kim-reynolds-bans-tiktok-on-state-owned-devices/ (Iowa); https://apnews.com/article/kansas-tik-tok-ban-explainer-83ef9bc3ff44d90e7b0f54bd8f5228cb (Kansas); https://www.wkms.org/government-politics/2023-01-16/tiktok-banned-from-kentucky-government-devices (Kentucky); https://www.foxnews.com/us/louisianas-secretary-state-bans-tiktok-devices-issued-department-state (Louisiana); https://apnews.com/article/politics-maine-state-government-china-business-734ce1f1abde9c3b2a9c8172c6763d01 (Maine); https://thehill.com/policy/technology/3764025-hogan-orders-tiktok-ban-for-maryland-government-employees/ (Maryland); https://apnews.com/article/politics-mississippi-state-government-tate-reeves-business-b3658341702baf2a49ab0afbb618ee98 (Mississippi); https://www.kdrv.com/news/national/nevada-bans-tiktok-on-government-devices/article_03e9903f-9fd7-553f-8ddb-9d6e82fec880.html (Nevada); https://thehill.com/homenews/state-watch/3805699-nj-governor-bans-tiktok-on-state-devices/ (New Jersey); https://www.wbtv.com/2023/01/12/nc-gov-roy-cooper-signs-executive-order-initiating-ban-tiktok-wechat-state-devices/ (North Carolina); https://www.foxbusiness.com/technology/north-dakota-governor-bans-tiktok-app-executive-agencies (North Dakota); https://thehill.com/homenews/state-watch/3805512-ohio-joins-list-of-states-banning-tiktok-on-government-electronic-devices/ (Ohio); https://www.kjrh.com/news/local-news/oklahoma-gov-stitt-bans-tiktok-on-government-devices (Oklahoma); https://www.wyff4.com/article/tiktok-south-carolina-employees-state-devices/42157146 (South Carolina); https://apnews.com/article/south-dakota-bans-tiktok-from-state-devices-f7a95dd494dab9c410ff80c577c609dd (South Dakota); https://www.nbcdfw.com/news/local/texas-news/gov-abbott-bans-tiktok-on-state-issued-laptops-phones-and-other-devices/3143349/ (Texas); https://thehill.com/homenews/state-watch/3772150-utah-governor-orders-tiktok-ban-for-state-government-employees/ (Utah); https://vtdigger.org/2023/02/20/vermont-state-government-bans-tiktok-on-its-devices/ (Vermont); https://thehill.com/homenews/state-watch/3778557-youngkin-joins-gop-governors-in-banning-tiktok-on-state-devices-wireless-networks/ (Virginia); https://www.jsonline.com/story/news/politics/2023/01/12/tony-evers-issues-order-banning-tiktok-on-some-state-issued-devices/69803482007/ (Wisconsin); https://cowboystatedaily.com/2022/12/15/wyoming-gov-mark-gordon-bans-tiktok-on-all-state-owned-devices/ (Wyoming); https://www.npr.org/2023/08/17/1194422613/new-york-city-bans-tiktok-

28. In February 2023, Senators Richard Blumenthal and Jerry Moran signed a joint letter demanding that the government impose a wall between Defendant TikTok Inc.'s U.S. operations and its Chinese parent company, Beijing ByteDance.[21] Senators Blumenthal and Moran expressed "profound concern regarding the risks that TikTok poses to our national security and to consumer privacy" given TikTok's collection of "sensitive information of tens of millions of American users."[22] Senators Blumenthal's and Moran's letter further recognized that "TikTok does not only collect the information regarding registered users" and that "the transmission to TikTok of non-user IP addresses, a unique ID number, and information about what an individual is doing on a site provides a deep understanding of those individuals' interests, behaviors, and other sensitive matters."[23] The Senators emphasized that "***even Americans who are not using the [TikTok] platform are at risk of having their information collected by TikTok.***"[24]

29. Senator Michael Bennet has urged TikTok Inc.'s CEO Shou Zi Chew "to consider his platform's harm to a generation of Americans."[25] Senate majority leader Chuck Schumer has indicated that the Senate Commerce Committee is currently conducting a review of the TikTok app and that a ban on the TikTok app "should be looked at."[26]

30. Public concern and scrutiny on TikTok, specifically in regards to its interception, collection and storage of data on ordinary Americans and the

---

government-devices (New York City).

[21] https://www.nbcnews.com/politics/congress/congress-tiktok-ban-social-media-harms-teens-rcna70998

[22] https://www.blumenthal.senate.gov/imo/media/doc/20230216cfiustiktok.pdf

[23] *Id.*

[24] *Id.* (emphasis added).

[25] *Id.*

[26] https://www.cnn.com/2023/02/12/tech/tiktok-us-ban-consideration-chuck-schumer/index.html

accessibility of that data in China, remains high. For instance, in June 2022, FCC Commissioner Brendan Carr urged the CEOs of Apple and Google to remove the TikTok app from their app stores. In his letter, Commissioner Carr emphasized that the TikTok app "collects vast troves of sensitive data about those U.S. users" and that "ByteDance officials in Beijing have repeatedly accessed the sensitive data that TikTok has collected from Americans after those U.S. users downloaded the app."[27]

31. In March 2023, Congress held a series of hearings regarding TikTok's collection of private data, its ties to the Chinese government, and the potential national security threat to the United States. At these hearings, FBI Director Christopher Wray testified that TikTok was "ultimately within the control of the Chinese government," and that TikTok's activity in the United States "screams out with national security concerns[.]"[28] NSA Director Paul Nakasone likened the threat posed by TikTok to a "loaded gun."[29] Nakasone has also cautioned that control of the private data collected by TikTok would provide the Chinese government with "a platform for information operations [and] a platform for surveillance" against the United States.[30]

32. Investigative reporting also continues to reinforce the threat that TikTok poses to the data of ordinary Americans. On May 24, 2023, the NEW YORK TIMES reported that TikTok employees share user data, including "the driver's licenses of American users," on Lark, an internal messaging and collaboration tool that TikTok uses.[31] Such data on ordinary Americans was posted to employee chat rooms within

---

[27] https://twitter.com/BrendanCarrFCC/status/1541823585957707776

[28] https://www.reuters.com/technology/fbi-chief-says-tiktok-screams-us-national-security-concerns-2023-03-08/

[29] https://www.reuters.com/video/watch/idOV611709032023RP1

[30] https://www.defense.gov/News/News-Stories/Article/Article/3354874/leaders-say-tiktok-is-potential-cybersecurity-risk-to-us/

[31] https://www.nytimes.com/2023/05/24/technology/inside-how-tiktok-shares-user-data-lark.html

Lark that could be accessed by thousands of chat room members, including "ByteDance workers in China and elsewhere."[32]

33. In June 2023, Senators Marsha Blackburn and Richard Blumenthal expressed disappointment at "TikTok's pattern of misleading or inaccurate responses regarding serious matters related to users' safety and national security."[33] In light of "recent reports that TikTok allowed private data about American users to be stored and accessed in China, despite repeated public assurances and Congressional testimony that TikTok data was kept in the United States," the two Senators requested that "TikTok correct and explain its previous, incorrect claims."[34]

34. In the face of ongoing public concern and scrutiny, TikTok has emphasized its "initiative to strengthen TikTok's data protection policies and protocols, further protect our users, and build confidence in our systems and controls in the United States."[35] By TikTok's own admission, however, it wasn't until January 2023 that "all new protected data is stored exclusively within" the United States.[36]

---

[32] *Id.*; *see also* Emily Baker-White, "TikTok Parent ByteDance Planned to Use TikTok to Monitor the Physical Location of Specific American Citizens," *Forbes* (Oct. 20, 2022), https://www.forbes.com/sites/emilybaker-white/2022/10/20/tiktok-bytedance-surveillance-american-user-data (ByteDance's Beijing-based Internal Audit and Risk Control department "planned to collect TikTok data about the location of a U.S. citizen").

[33] https://www.blackburn.senate.gov/services/files/76E769A8-3EDA-4BA0-989E-42D5F99E547D

[34] *Id*. After Senators Blackburn and Blumenthal flagged the discrepancies between TikTok's public representations and reporting on TikTok's data collection and storage practices, TikTok attempted to reconcile the two by distinguishing between data of TikTok users and TikTok creators. https://www.forbes.com/sites/alexandralevine/2023/06/21/tiktok-confirms-data-china-bytedance-security-cfius/?sh=5c6ddb593270. The data of the latter group, including social security numbers and tax IDs, are stored on servers in China. https://www.forbes.com/sites/alexandralevine/2023/05/30/tiktok-creators-data-security-china/?sh=7dcdee6a7048.

[35] https://www.blackburn.senate.gov/services/files/A4595D03-689A-43FF-ADBA-32C557DE3685

[36] *Id.*

Further, while TikTok apparently "began the process of deleting historic protected data globally" as of March 2023, that process is not complete.[37] Upon information and belief, sensitive data on Americans still remains stored on servers outside the United States and is accessible by Defendants' employees located in China.

35. Meanwhile, journalists continue to sound the alarm on the control and influence that TikTok's China-based parent company has over it. As recently as September 27, 2023, the WALL STREET JOURNAL reported on the transfer of senior executives from ByteDance's Beijing headquarters to TikTok in the United States, some of whom have brought their teams from Beijing. "TikTok has also consolidated some of its teams under the new leaders from ByteDance," and some U.S.-based TikTok employees "say they are worried that the appointments show ByteDance plays a greater role in TikTok's operations than TikTok has disclosed publicly."[38]

36. As discussed in the myriad public statements and news articles above, Defendants' mass collection of private data from ordinary Americans poses a unique national security threat due to the fact that Defendants are effectively controlled by the Chinese government. The strategic utility of this data is not limited to the individual level – *i.e.* for surveillance or blackmail of government employees and other individuals in key positions. It also exists on the aggregate level: the more the Chinese government knows about the behaviors and opinions of ordinary Americans, the more effectively it can influence the behaviors and opinions of the American public as a whole.

37. This is no idle concern: it is well-documented that since at least 2019, the Chinese government has been conducting "influence operations" through social

[37] *Id.*

[38] https://www.wsj.com/tech/tiktok-employees-say-executive-moves-to-u-s-show-china-parents-influence-ef5ff21f?mod=hp_lead_pos2. The *Wall Street Journal* further reported that U.S. employees "are compared with employees in China" for their performance reviews and that TikTok employees were instructed to "downplay the parent company ByteDance" and "downplay the China association." *Id.*

media and other large-scale "disinformation networks" in order to "exploit[] political polarization, the COVID-19 pandemic, and other issues and events to support its soft power agenda" in the U.S. and other democracies.[39] The more information China has on what news headline will make an American more likely to click on or share a news article, or what type of advertisement is more likely to make an American visit a particular website, the more tailored and effective its influence operations become.

38. Unsurprisingly, the American public has grown increasingly distrustful of Defendants' business practices. 59% of respondents to a February 2023 Harvard CAPS/Harris national poll said they believed that the TikTok app "is a medium the Chinese use to spy on Americans."[40] 42% said they would support a nationwide TikTok ban on privacy and security grounds.[41] Only 12% said they would allow the continued use of the TikTok app in the United States without conditions.[42]

B. Cookies and SDKs

39. The TikTok SDK represents the next step in Defendants' data harvesting campaign aimed at U.S. residents. Defendants have developed software that can and does illicitly harvest private and personally identifiable data, such as the webpages visited by users, search queries, User IDs, User Agent, phone numbers, email addresses, IP addresses, and more (collectively "Private Data") from users of websites with the TikTok SDK installed. Defendants have the ability to invade the privacy of unsuspecting U.S. residents who do not use the TikTok app, as these non-TikTok users go about their everyday business on websites that have no visible affiliation whatsoever to Defendants.

---

[39] https://www.rand.org/blog/2023/10/dismantling-the-disinformation-business-of-chinese.html

[40] https://harvardharrispoll.com/key-results-february-3/

[41] *Id.*

[42] *Id.*

40. An SDK—short for "software development kit"—is a package of pre-built software tools that allows developers to implement certain functionality on their platforms without the need to re-build code from the ground up.

41. Much modern software leverages SDKs from large software companies such as Google, Apple, or Microsoft, so that developers can implement basic functions "out of the box" with a simple download and installation, rather than having to "reinvent the wheel" every time for new software. For example, an "in-app billing" SDK can be used to implement billing functions, and an "advertising" SDK can be used to display ads on websites.

42. In particular, SDKs have become increasingly popular for web advertising. Once installed onto a particular website, advertising SDKs allow a website to connect to a larger ad network—such as Google AdSense or Facebook Ads—which allows them to serve personalized ads to users, and also collect some user data to send back to the ad network. Websites are compensated in the form of a share of the ad revenue from the network, based on the amount of traffic driven from the website to the network's ads.

43. Advertising SDKs can deliver personalized ads because they collect user data through "cookies." Cookies are small computer files that are automatically generated when a user visits a website, comprised of strings of text that contain information, such as user IDs, emails, or IP addresses. Every time a user visits the website, the cookie on the user's hard drive is passed back to the website for identification purposes. Cookies were originally developed to enable basic functionality requiring user identification, such as automatic log-ins, or saving your shopping cart on an e-commerce website. As technology has advanced, however, so too has the scope of the information collected by cookies.

44. In general, cookies are categorized by (1) the length of time for which they are placed on a user's device, and (2) the party who places the cookie on the user's device. "Session cookies" are placed on the user's computer for the time period

in which the user is reading and navigating the website that placed the cookie. Web browsers normally delete session cookies when the user closes the browser. "Persistent cookies" are designed to survive past one browser session of a user. The lifespan of a persistent cookie is set by the person who creates the cookie. As a result, a "persistent cookie" could stay on a user's device for years. Persistent cookies can be used to track users' actions on the Internet, and are also sometimes referred to as "tracking cookies."

C. Defendants use the TikTok SDK to secretly intercept and collect Private Data from unsuspecting U.S. residents browsing websites seemingly unrelated to TikTok

45. The TikTok SDK, which consists of at least the Pixel and Events API, is a new enterprise solution developed by Defendants and distributed under their "TikTok for Business" product line. Defendants market the TikTok SDK as a means to deliver more effective targeted ads—thus increasing ad revenue for websites that choose to install the TikTok SDK.

46. Although Defendants market the TikTok Pixel (sometimes referred to herein as "Pixel") as a means to deliver more effected targeted ads, the Pixel intercepts and collects Private Data even when that website does not run ads with TikTok. Indeed, Defendants allow a Pixel code to be generated even for a website that does not run ads with TikTok and even without configuring any events or settings for that Pixel.

47. Specifically, Defendants have designed the TikTok Pixel such that regardless of configuration, it will always collect full-string URLs from website visitors. This is because, by default, the TikTok Pixel is set to track any "PageView event," which transmits full-string URLs to Defendants. For the Pixel, as of October 2023, Defendants provide no way for websites to remove or deselect the tracking of PageView events. In other words, ***the collection of full-string URLs is a non-negotiable component of the TikTok Pixel.***

48. Upon information and belief, earlier iterations of the Pixel around 2021 also pre-configured the Pixel base code with the default PageView event but gave websites the option to deselect it. By eliminating the option to deselect PageView, Defendants have made the TikTok Pixel even more invasive of Private Data and have further decreased non-TikTok websites' autonomy to configure the code.

49. Once the baseline Pixel code (again, with no events configured other than the PageView that Defendants mandate as a default) is embedded on a website, it automatically transmits the following data to TikTok:

- **Timestamp**, or the time that the Pixel event fired, which is used to determine when website actions took place, like when a page was viewed or when a product was purchased.
- **User Agent**, which is used to determine the device make, model, operating system, and browser information.
- **URL**, which is the full-string URL of the webpage that the visitor is viewing, including the full document path with folder and subfolder structure.
- **Referrer URL**, which is the previously visited webpage.
- **User language**, which is the language that the server is expected to send back.
- **Pixel Session ID**, which is generated on the website and saves event information about a visitor's single visit.[43]

50. Defendants designed the Pixel to indiscriminately collect this baseline data, which includes full-string URLs, whether or not the non-TikTok website actually advertises with TikTok and whether or not the non-TikTok website has configured any events on which it seeks to collect information.

51. This nonnegotiable, baseline data collected by the Pixel consist of private and personally identifiable information. In particular, the full-string URL reveals an incredible amount of private and personally identifiable information. For

[43] https://ads.tiktok.com/help/article/using-cookies-with-tiktok-pixel?lang=en

instance, the URL of a "thank you" page to which a non-TikTok website visitor is directed after making a donation on a webpage could include private information like the visitor's email, country, amount of donation, and payment method. The URL of a non-TikTok webpage on which you order food for delivery, like Grubhub, could include the website visitor's address converted to a latitude-longitude value. And the URL of a "manage your booking" page after purchasing a train or flight ticket could include tokens that are unique to the visitor, like her username and password.[44]

52. In addition to the PageView event which Defendants have pre-configured without giving non-TikTok websites the option of deleting, Defendants also encourage non-TikTok websites to configure yet additional "events" with the TikTok Pixel. Defendants provide fourteen standard events that non-TikTok websites can add: Add Payment Info, Add to Cart, Add to Wishlist, Click Button, Complete Payment, Complete Registration, Contact, Download, Initiate Checkout, Place an Order, Search, Submit Form, Subscribe, and View Content.[45]

53. Defendants have further designed the TikTok Pixel so that when one visits a non-TikTok website that has the TikTok Pixel installed, two cookies are downloaded onto one's hard drive: a "first-party" cookie that is initially accessible by only the non-TikTok website, and a "third-party" cookie that is accessible directly by Defendants. These cookies store a broad range of personal information.

54. The "third-party" cookies are downloaded onto a user's computing device from each website where the TikTok Pixel is installed, allowing Defendants to keep track of and monitor an individual user's web activity over multiple non-TikTok websites.

55. Third-party cookies are used to help create detailed profiles on individuals, including but not limited to an individual's unique ID number, IP

[44] https://medium.com/hackernoon/watching-them-watching-us-how-websites-are-leaking-sensitive-data-to-third-parties-7a79fc549c6e

[45] https://ads.tiktok.com/help/article/standard-events-parameters?lang=en

address, browser, screen resolution, search terms, and a history of all non-TikTok websites visited within Defendants' TikTok Pixel network of websites. This allows Defendants to track the web activity of an individual and build a digital dossier.

56. Web browsers—such as Apple Safari, Microsoft Internet Explorer, Google Chrome, and Mozilla Firefox—have privacy settings that provide website visitors with the ability to block third-party cookies. For example, under the "Privacy and Security" settings in Google Chrome, visitors have the option to "Block third-party cookies."

57. Yet, where a web browser or operating system is set to block third-party cookies to prevent Defendants from obtaining Private Data, or where a website visitor rejects third-party cookies on the website's cookie banner, Defendants circumvent those settings to obtain Private Data anyway. The TikTok Pixel circumvents web browser and system settings by causing the non-TikTok website to share the first-party cookie with Defendants, in effect transmuting a first-party cookie into a third-party cookie with the ability to evade web browser and operating system settings that would otherwise block it from reaching Defendants.

58. Defendants have devised yet another way to circumvent browser or operating system settings to block cookies. This is where the TikTok Events API comes in. The Events API is software that websites can install on their servers to transmit even more non-TikTok website visitor data to Defendants. Because the Events API is installed on the non-TikTok websites' servers, rather than on the non-TikTok websites themselves, it can override non-TikTok website visitors' wishes to block cookies and thereby intercept, collect, and transmit their Private Data to Defendants anyway.

59. Defendants tout that the Pixel is an "out-of-the-box solution" with "no tech experience required."[46] "Coding is optional – anyone can set up website tracking

[46] https://www.tiktok.com/business/en-US/blog/get-started-with-tiktok-pixel

directly in TikTok Ads Manager with just a few clicks."[47] As demonstrated by the excerpt from Defendants' website below, Defendants actively encourage non-TikTok websites to install both the Pixel and Events API together.[48]

Compare Web Conversion Setup Methods

There are three ways to set up Web Conversion with TikTok, by utilizing Pixel, Events API, or both. Please see below the benefits of these setup scenarios:

	Events API	Pixel	Pixel + Events API (RECOMMENDED)
Benefits	- Enables more sustainable event sharing between your business and TikTok. - Improves ad delivery and targeting by capturing missed conversions - More control over what data your business shares with kTok.	- Lightweight implementation. - Easy customer event capture and reporting. - Automatic updates to pixel performance included.	- Events API enriches conversions shared by Pixel. - Enriched conversions enhances full-funnel measurement, ad delivery, and audience creation. - Enables sustainable transition to ad industry changes.

60. At least 500,000 non-TikTok websites, including a large number that are widely used, have installed the TikTok SDK, thereby allowing Defendants to obtain Private Data from visitors of these non-TikTok websites. Having never used the TikTok app or registered for a TikTok account, a multitude of these visitors never had any notice—actual or constructive—of TikTok's privacy policy or terms of use, and never consented to Defendants' interception and collection of their Private Data. By aggregating Private Data over a wide range of non-TikTok websites, Defendants assemble a comprehensive profile of these non-TikTok users.

61. For example, CONSUMER REPORTS recently revealed that:

> The national Girl Scouts website has a TikTok pixel on every page, which will transmit details about children if they use the site. TikTok gets medical information from WebMD, where a pixel reported that we'd searched for "erectile dysfunction." And RiteAid told TikTok when we added Plan B emergency contraceptives to our cart. Recovery Centers of America, which operates addiction treatment facilities,

[47] *Id.*

[48] https://ads.tiktok.com/help/article/events-api?lang=en

notifies TikTok when a visitor views its locations or reads about insurance coverage.[49]

62. The CONSUMER REPORTS article quotes a TikTok spokesperson, Melanie Bosselait, as admitting that when "TikTok receives data about someone who doesn't have a TikTok account, the company only uses that data for aggregated reports that they send to advertisers about their websites."[50]

63. In dozens of countries, Defendants have been growing their footprint to provide ads on non-TikTok websites and apps as well. As one example, Defendants have released a product called Pangle, which Defendants market as "the ad network of TikTok for Business," and tout that it "enables advertisers to effectively reach broad audiences by running ads in placements on 3rd party apps."[51] Defendants have released Pangle in over 30 countries, including Canada and Mexico. In addition, Defendants have released another product called Global App Bundle, which allows advertisers to place ads on non-TikTok apps released by ByteDance, including CapCut and Fizzo. Defendants tout that the Global App Bundle "gives advertisers access to additional audiences beyond TikTok."[52] In short, Defendants now develop and market products that display ads to non-TikTok users.

64. THE VERGE recently reported that Cerebral, a telehealth startup specializing in mental health, shared sensitive data of over 3.1 million patients with TikTok through its use of "tracking pixels." The sensitive patient data collected through the TikTok Pixel "includes everything from patient names, phone numbers, email addresses, birth dates, IP addresses, insurance information, appointment dates, treatment" and may even include "the answers clients filled out as part of the mental

[49] https://www.consumerreports.org/electronics-computers/privacy/tiktok-tracks-you-across-the-web-even-if-you-dont-use-app-a4383537813/

[50] *Id.*

[51] https://ads.tiktok.com/help/article/pangle-placement?lang=en

[52] https://ads.tiktok.com/help/article/global-app-bundle-placement

health self-assessment on the company's website and app, which patients can use to schedule therapy appointments and receive prescription medication."[53]

65. The TikTok Pixel's growing ubiquity is also confirmed by a WALL STREET JOURNAL report that the Pixel was found on "more than two dozen" official websites of state governments, including governments that have banned the TikTok app from government devices.[54] "The presence of that code means that U.S. state governments around the country are inadvertently participating in a data-collection effort for a foreign-owned company, one that senior Biden administration officials and lawmakers of both parties have said could be harmful to U.S. national security and the privacy of Americans."[55]

66. The TikTok SDK can also be used for purposes of digital "fingerprinting." As explained by WIRED:

> The exact configuration of lines and swirls that make up your fingerprints are thought to be unique to you. Similarly, your browser fingerprint is a set of information that's collected from your phone or laptop each time you use it that advertisers can eventually link back to you.
>
> "It takes information about your browser, your network, your device and combines it together to create a set of characteristics that is mostly unique to you," says Tanvi Vyas, a principal engineer at Firefox. The data that makes up your fingerprint can include the language you use, keyboard layout, your timezone, whether you have cookies turned on, the version of the operating system your device runs, and much more.
>
> By combining all this information into a fingerprint, it's possible for advertisers to recognize you as you move from one website to the next. Multiple studies looking at fingerprinting have found that around 80 to 90 percent of browser fingerprints are unique. Fingerprinting is often done by advertising technology companies that insert their code onto websites. Fingerprinting code—which comes in the form of a variety of scripts, such as the FingerprintJS library—is deployed by dozens of ad tech firms to collect data about your online activity. Sometimes websites that have fingerprinting scripts on them don't even know about it. And the companies are often opaque and unclear in the ways they track you.

[53] https://www.theverge.com/2023/3/11/23635518/cerebral-patient-data-meta-tiktok-google-pixel

[54] https://www.wsj.com/articles/tiktok-trackers-embedded-in-u-s-state-government-websites-review-finds-a2589f0

[55] *Id.*

> Once established, someone's fingerprint can potentially be combined with other personal information—such as linking it with existing profiles or information murky data brokers hold about you. "There are so many data sets available today, and there are so many other means to connect your fingerprint with other identifying information," says Nataliia Bielova, a research scientist at France's National Institute for Research in Digital Science and Technology, who is currently working at the French data regulator, CNIL.[56]

67. Upon information and belief, Defendants are able to associate the information they obtain through the unconsented to and undisclosed data interception and collection described herein with personally identifying information of non-TikTok users. Defendants are able to accomplish this through, among other things, "digital fingerprinting" techniques.

68. Defendants' audacious invasion of privacy without notice to or the authorization of Plaintiffs and Class and Subclass members is motivated, in part, by their effort to improve their own algorithms and technology. The explosive growth in the popularity of the TikTok app—and attendant growth in advertising revenue for Defendants—is attributable, in part, to the TikTok app's ability to predict the interests of its users. This capability is powered by an algorithm that has benefited from a mountain of data—regardless of whether it comes from TikTok or non-TikTok users—collected by Defendants. Defendants use the illicitly collected data to improve their own algorithms and technology. Non-TikTok websites from which Defendants surreptitiously intercept and collect Private Data through the TikTok

[56] https://www.wired.com/story/browser-fingerprinting-tracking-explained/; *see also* https://www.wsj.com/articles/tiktok-trackers-embedded-in-u-s-state-government-websites-review-finds-a2589f0 ("While the web-tracking pixels ostensibly aim to better pinpoint advertising, they also pose threats for privacy, security experts have said. They can sometimes be configured to collect data that users enter on websites, such as usernames, addresses and other sensitive information. With enough pixels on enough websites, the companies running them can begin to piece together the browsing behavior of individual users as they move from domain to domain, building detailed profiles on their interests and online habits.").

SDK include such popular and widely known websites as streaming video service Hulu, e-commerce platform Etsy, freelancing platform Upwork, and Build-a-Bear Workshop, a custom teddy bear design shop for children.

69. Defendants have also intercepted and collected Private Data from non-TikTok websites where visitors' search and browse history is likely to disclose sensitive information. This includes: (1) websites relating to personal health information, such as Rite Aid, The Vitamin Shoppe, WebMD, Weight Watchers, The Planned Parenthood Federation of America, Cerebral, and Recovery Centers of America; (2) websites relating to sensitive financial information, such as SmartAsset and Happy Money; (3) religious websites, such as the United Methodist Church; and (4) websites that may disclose the activities of minor children, such as the Girl Scouts of the USA.

70. Critically, Defendants have also intercepted and collected Private Data from some government websites, including the COVID-19 information page of the Maryland Department of Health,[57] and the Arizona Department of Economic Security.[58]

71. These are just a few examples of the 500,000 or more non-TikTok websites that have become Trojan horses for Defendants to steal Private Data from non-TikTok users in the United States.

D. Plaintiffs' and Class and Subclass members' Private Data has economic value, and there is a market for such Private Data

72. The value of personal data is well understood and generally accepted as a form of currency.

[57] https://www.wsj.com/articles/tiktok-trackers-embedded-in-u-s-state-government-websites-review-finds-a2589f0

[58] https://www.consumerreports.org/electronics-computers/privacy/tiktok-tracks-you-across-the-web-even-if-you-dont-use-app-a4383537813/

73. It is by now incontrovertible that a robust market for this data undergirds the tech economy.

74. The robust market for Internet user data has been analogized to the "oil" of the tech industry.[59] A 2015 article from TechCrunch accurately noted that "Data has become a strategic asset that allows companies to acquire or maintain a competitive edge."[60] That article noted that the value of a single Internet user—or really, a single user's data—varied from about $15 to more than $40.

75. The Organization for Economic Cooperation and Development ("OECD") itself has published numerous volumes discussing how to value data such as that which is the subject matter of this Complaint, including as early as 2013, with its publication "Exploring the Economic of Personal Data: A Survey of Methodologies for Measuring Monetary Value."[61] The OECD recognizes that data is a key competitive input not only in the digital economy but in all markets: "Big data now represents a core economic asset that can create significant competitive advantage for firms and drive innovation and growth."[62]

76. In *The Age of Surveillance Capitalism*, Harvard Business School Professor Shoshanna Zuboff notes that large corporations like Verizon, AT&T and Comcast have transformed their business models from fee for services provided to customers to monetizing their user's data—including user data that is not necessary for product or service use, which she refers to as "behavioral surplus."[63] In essence,

---

[59] https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

[60] https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/

[61] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD DIGITAL ECONOMY PAPERS, No. 220 (Apr. 2, 2013), https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf

[62] https://www.oecd-ilibrary.org/industry-and-services/supporting-investment-in-knowledge-capital-growth-and-innovation_9789264193307-en

[63] Shoshanna Zuboff, THE AGE OF SURVEILLANCE CAPITALISM 166 (2019)

Professor Zuboff explains that revenue from Internet user data pervades every economic transaction in the modern economy. It is a fundamental assumption of these revenues that there is a *market* for this data; data generated by Internet users on non-TikTok websites in which the TikTok SDK is installed has economic value.

77. Professor Paul M. Schwartz, writing in the HARVARD LAW REVIEW, notes: "Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information."[64]

78. As Professors Acquisti, Taylor, and Wagman relayed in their 2016 article "The Economics of Privacy," published in the JOURNAL OF ECONOMIC LITERATURE: "Such vast amounts of collected data have obvious and substantial economic value. Individuals' traits and attributes (such as a person's age, address, gender, income, preferences, and reservation prices, but also her clickthroughs, comments posted online, photos uploaded to social media, and so forth) are increasingly regarded as business assets that can be used to target services or offers, provide relevant advertising, or be traded with other parties."[65]

79. There is also a private market for Internet users' personal information. While there is a wide range in values, the prices are nonetheless significant. For example:

- According to the OECD, in the United States, an individual's address is available for purchase at $0.50, a birthdate at $2, a social security number for $8, a driver's license number at $3, and a military record at $35).[66]

[64] Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2055, 2056-57 (2004)

[65] Alessandro Acquisti, Curtis Taylor, and Liad Wagman, *The Economics of Privacy*, 54 J. of Econ. Literature 2, at 444 (June 2016), https://www.heinz.cmu.edu/~acquisti/papers/AcquistiTaylorWagman-JEL-2016.pdf

[66] *Exploring the Economics of Personal Data: A Survey of Methodologies for*

- "Each piece of personal info has a price tag. A Social Security number may sell for as little as $1. Credit card, debit card and banking info can go for as much as $110. Usernames and passwords for non-financial institution logins are $1, but it can range from $20 to $200 for login info for online payment platforms."[67]

- "Researchers pored through the prices of personal data and information—called 'fullz' by those searching for 'full credentials'—that are available for sale on nearly 50 different Dark Web marketplaces, finding that Japan, the UAE, and EU countries have the most expensive identities available at an average price of $25."[68]

- "According to Comparitech, who researched the prices of stolen credit cards, hacked PayPal accounts, and private Social Security numbers on more than 40 different dark web marketplaces, the average price of each U.S. citizen's "fullz," or complete information including name, date of birth, address, phone number, account numbers and other information is $8."[69]

80. These rates are assumed to be discounted because they do not operate in competitive markets, but rather, in an illegal marketplace. If a criminal can sell other Internet users' stolen data, surely Internet users can sell their own data.

81. In short, there is a quantifiable economic value to Internet users' data that is greater than zero. The exact number will be a matter for experts to determine.

82. Historically, this economic value has been leveraged largely by corporations who pioneered the methods of its extraction, analysis, and use. However, the data also has economic value to Internet users. Market exchanges have sprung up where individual users like Plaintiffs herein can sell or monetize their own data. As non-exhaustive examples:

- Google runs a "Screenwise Panel" through market research company Ipsos,

Measuring Monetary Value, OECD DIGITAL ECONOMY PAPERS, No. 220 (Apr. 2, 2013) at 5, https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf

[67] https://www.onpointcu.com/blog/understanding-the-illegal-market-for-personal-information/#:~:text=Each%20piece%20of%20personal%20info,info%20for%20online%20payment%20platforms

[68] https://www.techrepublic.com/article/how-much-is-your-info-worth-on-the-dark-web-for-americans-its-just-8/

[69] https://vmits.com/theres-value-in-everything-stop-underestimating-the-value-of-your-data-on-the-black-market/

which is designed to learn more about how everyday people use the Internet. In exchange for adding a browser extension that shares with Google the sites they visit and how they use them, Google pays selected participants in gift cards to retailers like Barnes & Noble and Walmart.

- Brave's web browser pays users to watch online targeted ads, while blocking out everything else.[70]
- Loginhood "lets individuals earn rewards for their data and provides website owners with privacy tools for site visitors to control their data sharing," via a "consent manager" that blocks ads and tracking on browsers as a plugin.[71]
- Killi, a data exchange platform, allows you to own and earn from your data.[72]
- BIGtoken, another "platform to own and earn from your data," allows you to "use the BIGtoken application to manage your digital data and identity and earn rewards when your data is purchased."[73]
- The Nielsen Company's Nielsen Computer and Mobile Panel will pay you to install its tracking application on your computer, phone, tablet, e-reader, or other mobile device.[74]
- Zynn, a TikTok competitor, pays users to sign up and interact with the app.[75]
- Consumer focus groups and surveys also pay participants for information on their preferences.

83. There are countless examples of this kind of market, and the desire for individuals to participate directly is growing more robust as information asymmetries are diminished through revelations to users as to how their data is being collected

[70] https://lifehacker.com/get-paid-towatch-ads-in-the-brave-web-browser-1834332279#:~:text=Brave%2C%20a%20chromiumbased%20web%20browser%20that%20boasts%20an,a%20more%20thoughtful%20way%20than%20we%E2%80%99re%20accustomed%20to

[71] https://loginhood.io/product/chrome-extension ("[s]tart earning rewards for sharing data – and block others that have been spying on you. Win-win.").

[72] https://killi.io/earn/.

[73] https://bigtoken.com/faq#general_0 ("Third-party applications and sites access BIGtoken to learn more about their consumers and earn revenue from data sales made through their platforms. Our BIG promise: all data acquisition is secure and transparent, with consumers made fully aware of how their data is used and who has access to it.").

[74] https://wallethacks.com/apps-for-selling-your-data/

[75] https://www.theverge.com/2020/5/29/21274994/zynn-tiktok-clone-pay-watch-videos-kuaishou-bytedance-rival

and used. Individuals—including Plaintiffs—now increasingly recognize that the personal information they furnish to companies holds value and actionable insights, enabling firms to sculpt effective business strategies.[76]

84. However, recent years have witnessed a notable transition in private data collection methodologies. The traditional avenues, such as surveys, have experienced a decline as more advanced and automated techniques gain traction.[77] The shift was propelled by market conditions that necessitate novel approaches to engage individuals, resulting in a diminished reliance on surveys and an uptick in real-time consumer data harvesting through various online platforms,[78] the very sort of harvesting that TikTok is engaged in here.

85. A stark contrast exists between the modus operandi of data collection today as compared to the past. Unlike surveys, contemporary data harvesting often occurs without explicit consent and devoid of any compensatory offer to the consumer. This method proves to be a more lucrative and higher return on investment for entities as opposed to the earlier practice of crafting surveys, disseminating them, and compensating the respondents.[79]

86. Defendants profit from this covert data-harvesting practice to the detriment of Plaintiffs and the Class and Subclass members. The market for personal data exists and is thriving, but individual consumers like Plaintiffs and the Class and

---

[76] Roger Horberry, *Why Your Market Research Team is More Valuable Than Ever*, GLOBALWEBINDEX (February 3, 2021), https://blog.gwi.com/marketing/market-research-more-valuable-than-ever/ (last visited Oct. 5, 2023).

[77] *See generally* Lorena Blasco-Arcas ET AL., *The Role of Consumer Data in Marketing: A Research Agenda*, 146 J. BUS. RES. 436, 436-452 (2022).

[78] *Id.*

[79] *See generally* Michael McFarland, SJ, *Unauthorized Transmission and Use of Personal Data*, MARKKULA CENTER FOR APPLIED ETHICS AT SANTA CLARA UNIVERSITY, SCU, https://www.scu.edu/ethics/focus-areas/internet-ethics/resources/unauthorized-transmission-and-use-of-personal-data/ (last visited Oct. 5, 2023).

Subclass members have fewer opportunities to market their data for value, thereby diminishing the value of their data to them.

E. Plaintiffs and Class and Subclass members suffered an economic injury.

87. Property is the right of any person to possess, use, enjoy, or dispose of a thing, including intangible things such as data or communications.

88. California courts have recognized the lost "property value" of personal information. Recent changes in California law have also confirmed that individuals have a property interest in their information. In 2018, California enacted the California Consumer Privacy Act ("CCPA"). Among other things, the CCPA permits businesses to purchase consumer information from consumers themselves (Cal. Civ. Code § 1798.125(b)(1)) and permits businesses to assess and appraise—*i.e.*, to place a monetary value on—consumer data (Cal. Civ. Code § 1798.125(a)(2)).

89. The CCPA further provides consumers with the right to direct businesses to refrain from selling their personal information to third parties and prohibits businesses from discriminating against consumers for opting out from data collection. Cal. Civ. Code §§ 1798.120(a), 1798.125(a). Under the CCPA, personal data now encompasses the legal right to exclude others, which is an essential element of individual property.

90. Plaintiffs' and Class and Subclass members' Private Data is property under California law.

91. Defendants' interception, collection, and use of Plaintiffs' and Class and Subclass members' Private Data without authorization is a taking of Plaintiffs' and Class and Subclass members' property. Plaintiffs and Class and Subclass members have a right to disgorgement and/or restitution damages for the value of the improperly intercepted and collected Private Data by Defendants through the TikTok SDK.

92. Plaintiffs and Class and Subclass members have suffered damages, in that Defendants took more data than authorized. Those damages also include, but are not limited to: (i) loss of the promised benefits of their experience on the websites on which the TikTok SDK is installed; and (ii) loss of control over property which has marketable value.

93. To preserve their privacy, Plaintiffs and Class and Subclass members who now understand at least some of Defendants' violations are presented with the choice of (i) reducing or ending their participation with the websites on which the TikTok SDK is installed; or (ii) knowingly accepting less privacy than they were promised. Each of these options harms Plaintiffs and Class and Subclass members. There is no option that recovers the property improperly intercepted and collected by Defendants.

94. Further, Plaintiffs and Class and Subclass members were denied the benefit of knowing that Defendants were intercepting and collecting their Private Data. Thus, they were unable to mitigate the harms they incurred because of Defendants' actions. That is, Defendants' lack of transparency prevented and still prevents Plaintiffs' and Class and Subclass members' ability to mitigate the harms.

95. Defendants avoided costs they should have incurred because of their actions. Had they transparently disclosed their actions, they would have suffered losses stemming from the non-TikTok websites' loss of user engagement. Warning website visitors would have chilled engagement on the non-TikTok websites as well as discouraging potential new visitors, and thus chilled use of the TikTok SDK.

96. Defendants thus were not only able to evade or defer these costs, but they were able to continue to accrue value and further benefit from the delay in disclosing their actions (due to the time value of money). Defendants have thus transferred all of the costs imposed by the unauthorized interception and collection of non-TikTok users' Private Data onto Plaintiffs and Class and Subclass members. Defendants increased the cost to Plaintiffs and Class and Subclass members of

mitigating the interception and collection of their Private Data by failing to notify them that Defendants were intercepting and collecting Plaintiffs' and Class and Subclass members' Private Data.

97. In addition, Plaintiffs and Class and Subclass members have suffered from the diminished value of their own Private Data, which is property that has both personal and economic value to Plaintiffs and Class and Subclass members.

98. Plaintiffs' and Class and Subclass members' Private Data have different forms of value. First, there is transactional, or barter, value. Indeed, Defendants have traded (i) the ability to use non-TikTok websites with the TikTok SDK installed in exchange for (ii) the collection and use of Plaintiffs' and Class and Subclass members' Private Data—all while concealing the extent to which this information would be intercepted, collected, and used.

99. Second, Plaintiffs' and Class and Subclass members' property, which has economic value, was taken from them without their consent. There is a market for this Private Data, and it has at minimum a value greater than zero. The market value of Plaintiffs and Class and Subclass members' Private Data has been diminished because Defendants' improper interception, collection, and use of that Private Data means that Plaintiffs' and Class and Subclass members' Private Data is less marketable.

100. Third, in addition to the monetary value of selling their data, Plaintiffs and Class and Subclass members also assign value to keeping their Private Data private. It is possible to quantify this privacy value, which is destroyed when Defendants intercept and collect Plaintiffs' and Class and Subclass members' Private Data without notice or authorization.

101. Plaintiffs and Class and Subclass members were harmed when Defendants took their property and exerted exclusive control over it, intercepting and collecting it without Plaintiffs' and Class and Subclass members' knowledge to benefit Defendants and, additionally, for still undisclosed purposes.

102. Further, Defendants' control over these ever-expanding digital dossiers makes tracking and profiling Plaintiffs and Class and Subclass members much more efficient and effective. Defendants unjustly earn substantial profits from such targeted advertising and/or from the sale of user data and/or information or services derived from such data.

103. In sum, Defendants have intercepted and collected Plaintiffs' and Class and Subclass members' Private Data without providing anything of value to Plaintiffs and Class and Subclass members in exchange for that Private Data. Moreover, Defendants' unauthorized access to Plaintiffs' and Class and Subclass members' Private Data has diminished the value of that Private Data. These actions and omissions by Defendants have resulted in harm to Plaintiffs and Class and Subclass members.

V. DELAYED DISCOVERY AND TOLLING

104. Each unauthorized transmission of Private Data to Defendants by the TikTok SDK is a separate "wrong" which triggers anew the relevant statute of limitations.

105. Further, all applicable statutes of limitation have been tolled by operation of the delayed discovery doctrine, which delays accrual until Plaintiffs have, or should have, inquiry notice of the cause of action. Plaintiffs and Class and Subclass members were not on inquiry notice despite acting with reasonable diligence, for at least two reasons. First, because they have never been a registered user of the TikTok app or held any TikTok account, they would have no reason to suspect that TikTok would be intercepting and collecting their information from non-TikTok websites with no visible affiliation whatsoever with TikTok, or to inquire further as to that possibility. Second, even if they had inquired as to whether TikTok was collecting some information from non-TikTok websites, Plaintiffs would have to have special expertise in identifying and interpreting the underlying coding and

the operation of the TikTok SDK in order to discover Defendants' wrongful conduct. Plaintiffs lack this special expertise.

106. Plaintiffs did not discover and could not reasonably have discovered that Defendants were intercepting, collecting, storing, and using their Private Data in the ways set forth in this Complaint until they consulted with counsel—either shortly before the initial Class Action Complaint was filed in May 2023 (Plaintiff Griffith), or shortly before this First Amended Class Action Complaint was filed in October 2023 (the other Plaintiffs).

107. Upon learning about counsel's investigation into Defendants' improper interception, collection, storing, and use of their Private Data, Plaintiffs diligently sought to uncover the facts, including by consulting with, and hiring, knowledgeable counsel to bring this case.

VI. NAMED PLAINTIFF ALLEGATIONS

A. Bernadine Griffith

108. Plaintiff Bernadine Griffith is a resident of Riverside County, California. Ms. Griffith has never been a registered user of the TikTok app or held any TikTok account. She made a conscious decision not to do so because, like many other Americans, she was concerned that TikTok would violate her privacy.

109. Unbeknownst to Ms. Griffith, several of the non-TikTok websites that she frequently visited have installed the TikTok SDK. Defendants secretly intercepted and collected her Private Data from these websites through the TikTok SDK, including browsing history and search queries. This is precisely what Ms. Griffith wanted to avoid when she chose not to become a registered user of the TikTok app or hold any TikTok account.

110. For example, Ms. Griffith has on several occasions searched and browsed for both over-the-counter medication on the website of pharmacy chain Rite Aid, including within the past year. Ms. Griffith was able to search and browse for these medications without reviewing Rite Aid's privacy policies. The TikTok SDK

was installed on Rite Aid. Thus, unbeknownst to Ms. Griffith, when she visited Rite Aid, TikTok stole her Private Data through the TikTok SDK, including what medication she searched and browsed for. On information and belief, this information was personally identifiable.

111. Since 2017, Ms. Griffith has from time to time had paid subscriptions to the video-streaming service Hulu to watch her favorite television shows. Ms. Griffith was able to create Hulu accounts and watch content on Hulu without reviewing Hulu's privacy policies. Ms. Griffith visited Hulu frequently, and has done so as recently as the past month. The TikTok SDK was and is installed on Hulu. Thus, unbeknownst to Ms. Griffith, when she visited Hulu, Defendants stole her Private Data through the TikTok SDK. This includes information on what videos she searched for, browsed, and watched.

112. Since June 2018, Ms. Griffith has been a member of the e-commerce website Etsy. Ms. Griffith was able to create an Etsy account and to browse and shop on Etsy without reviewing Etsy's privacy policies. Ms. Griffith visited Etsy frequently, and has done so as recently as the past month. The TikTok SDK was and is installed on Etsy. Thus, unbeknownst to Ms. Griffith, when she visited Etsy, Defendants stole her Private Data through the TikTok SDK. This includes information on what products she searched for, browsed, purchased, and sold.

113. In or around early 2022, Ms. Griffith visited Build-a-Bear Workshop, a website that sells custom-made Teddy Bears. Ms. Griffith was able to browse on Build-a-Bear Workshop without reviewing its privacy policies. The TikTok SDK was and is installed on Build-a-Bear Workshop. Thus, unbeknownst to Ms. Griffith, every time she visited Build-a-Bear Workshop, Defendants stole her Private Data through the TikTok SDK. This includes information on what products she searched for, browsed, purchased, and sold.

114. Ms. Griffith is very conscious about her online privacy. She is a user of the Microsoft Edge and Google Chrome browsers. On both browsers, Ms. Griffith

has changed her settings to block third-party cookies and has enabled the "do not track" function. She also utilizes McAfee security software to protect her online privacy. Despite Ms. Griffith's efforts, the TikTok SDK circumvents these measures and obtains her Private Data, by among other things transmuting its third-party cookie into a first-party cookie.

115. During the Class Period, Ms. Griffith has marketed her Private Data at least by participating in several focus groups and surveys that compensated her for her participation. Ms. Griffith has participated in paid focus groups for consumer products like stoves and ovens, dog food, and curling irons. The value of Ms. Griffith's participation in these focus groups and surveys has been diminished due to the fact that Defendants make available extensive information about her consumer preferences and activity without compensating her in any way.

116. The Rite Aid, Hulu, Etsy, and Build-a-Bear Workshop websites are just some representative examples of non-TikTok websites where Defendants have stolen the Private Data of Ms. Griffith and Class and Subclass members. Upon information and belief, the TikTok SDK is installed on 500,000 non-TikTok websites, including many popular websites visited on a day-to-day basis by millions of Americans including Ms. Griffith and Class and Subclass members.

B. Patricia Shih

117. Plaintiff Patricia Shih is a resident of Orange County, California. Ms. Shih has never been a registered user of the TikTok app or held any TikTok account. She made a conscious decision not to do so because, like many other Americans, she was concerned that TikTok would violate her privacy.

118. Ms. Shih works remotely as a consultant for the Florida Department of Transportation. In this capacity, she has been provided with some access to the Florida Department of Transportation's internal network and private organizational accounts for ArcGIS and Microsoft Teams. While connected to the network, she has access to transportation management infrastructure. The network also shares traffic

and incident data bidirectionally with local government agencies. This network contains confidential information and is connected to various traffic systems, such as traffic cameras, sensors, and detectors. Because of this, Ms. Shih was required to obtain Criminal Justice Information Services Level 4 certification before being granted access. This certification required Ms. Shih to pass an exam and a background check.

119. Unbeknownst to Ms. Shih, several of the non-TikTok websites that she frequently visited have installed the TikTok SDK. Defendants secretly intercepted and collected her Private Data from these websites through the TikTok SDK, including browsing history and search queries. This is precisely what Ms. Shih wanted to avoid when she chose not to become a registered user of the TikTok app or hold any TikTok account.

120. For example, since March 2023, Ms. Shih has been a member of Upwork, a website that connects freelancers with job offers. Since then, Ms. Shih has on several occasions browsed and searched for various services and job offers on Upwork. She was able to do so without reviewing Upwork's privacy policies. The TikTok SDK was and is installed on Upwork. Thus, unbeknownst to Ms. Shih, when she visited Upwork, Defendants stole her Private Data through the TikTok SDK. This includes information on what services and job offers she searched or browsed for.

121. Ms. Shih is also a member of the Hulu website. In or around September 2023, Ms. Shih visited the Hulu website to search and browse for television shows. Ms. Shih was able to do so without reviewing Hulu's privacy policies. The TikTok SDK was and is installed on Hulu. Thus, unbeknownst to Ms. Shih, when she visited Hulu, Defendants stole her Private Data through the TikTok SDK. This includes information on what television shows she searched and browsed for.

122. In or around September 2023, Ms. Shih searched and browsed for products on e-commerce website Etsy. Ms. Shih was able to do so without reviewing Etsy's privacy policies. The TikTok SDK was and is installed on Etsy. Thus,

unbeknownst to Ms. Shih, when she visited Etsy, Defendants stole her Private Data through the TikTok SDK. This includes information on what products she searched and browsed for.

123. Ms. Shih is very conscious about her online privacy. She is a user of the Apple Safari and Google Chrome browsers. On both browsers, Ms. Shih has enabled the "do not track" function. She has all third-party cookies blocked on Safari, and has installed the Ghostery browser extension on her laptop to block third-party cookies and other trackers. Despite Ms. Shih's efforts, the TikTok SDK circumvents these measures and obtains her Private Data, by among other things transmuting third-party cookie into a first-party cookie.

124. During the Class Period, Ms. Shih has marketed her Private Data by participating in several phone surveys that compensated her for her participation. Ms. Shih has participated in surveys to rate the effectiveness of advertisements for consumer products, a survey asking her about wine preferences, two surveys asking for opinions on pet products, and a survey to measure her perception of various vacuum cleaner brands. Ms. Shih also participated in surveys conducted by SoCal Edison and Providence Health Services to measure public perception of those companies, including the effectiveness of various ad campaigns. The value of Ms. Shih's participation in these focus groups and surveys has been diminished due to the fact that Defendants make available extensive information about her consumer preferences and activity without compensating her in any way.

125. The Upwork, Hulu, and Etsy websites are just some representative examples of non-TikTok websites where Defendants have stolen the Private Data of Ms. Shih and Class and Subclass members. Upon information and belief, the TikTok SDK is installed on at least 500,000 non-TikTok websites, including many popular websites visited on a day-to-day basis by millions of Americans including Ms. Shih and Class and Subclass members.

C. Rhonda Irvin

126. Plaintiff Rhonda Irvin is a resident of Tulare County, California. Ms. Irvin has never been a registered user of the TikTok app or held any TikTok account. She made a conscious decision not to do so because, like many other Americans, she was concerned that TikTok would violate her privacy.

127. Unbeknownst to Ms. Irvin, several of the non-TikTok websites that she frequently visited have installed the TikTok SDK. Defendants secretly intercepted and collected her Private Data from these websites through the TikTok SDK, including browsing history and search queries. This is precisely what Ms. Irvin wanted to avoid when she chose not to become a registered user of the TikTok app or hold any TikTok account.

128. For example, Ms. Irvin is a member of The Vitamin Shoppe's website, where she has searched for, browsed, and purchased health supplements. Ms. Irvin was able to sign up for an account with The Vitamin Shoppe, and search for, browse, and purchase products without reviewing The Vitamin Shoppe's privacy policies. Ms. Irvin has visited The Vitamin Shoppe website frequently, and has done so as recently as two weeks ago. The TikTok SDK was installed on The Vitamin Shoppe website. Thus, unbeknownst to Ms. Irvin, when she visited The Vitamin Shoppe website, Defendants stole her Private Data through the TikTok SDK including what health supplements she purchased, searched for, and browsed. On information and belief, this information was personally identifiable.

129. Ms. Irvin is very conscious about her online privacy. She is a user of the Google Chrome browser, and utilizes McAfee security software.

130. The value of Ms. Irvin's Private Data has been diminished due to the fact that Defendants make available extensive information about her consumer preferences and activity without compensating her in any way.

131. The Vitamin Shoppe website is just a representative example of non-TikTok websites where Defendants have stolen the Private Data of Ms. Irvin and

Class and Subclass members. Upon information and belief, the TikTok SDK is installed on at least 500,000 non-TikTok websites, including many popular websites visited on a day-to-day basis by millions of Americans including Ms. Irvin and Class and Subclass members.

D. Matthew Rauch

132. Plaintiff Matthew Rauch is a resident of El Paso County, Texas. Mr. Rauch has never been a registered user of the TikTok app or held any TikTok account. He made a conscious decision not to do so because, like many other Americans, he was concerned that TikTok would violate his privacy.

133. Unbeknownst to Mr. Rauch, several of the non-TikTok websites that he frequently visited have installed the TikTok SDK. TikTok secretly intercepted and collected his Private Data from these websites through the TikTok SDK, including browsing history and search queries. This is precisely what Mr. Rauch wanted to avoid when he chose not to become a registered user of the TikTok app or hold any TikTok account.

134. For example, in or around November 2022, Mr. Rauch searched and browsed for over-the-counter medication on the website of pharmacy chain Rite Aid. Mr. Rauch was able to do so without reviewing Rite Aid's privacy policies. The TikTok SDK was installed on Rite Aid. Thus, unbeknownst to Mr. Rauch, when he visited Rite Aid, Defendants stole his Private Data through the TikTok SDK, including what medication he searched and browsed for.

135. Mr. Rauch has also searched and browsed for health supplements from The Vitamin Shoppe. Mr. Rauch was able to do so without reviewing The Vitamin Shoppe's privacy policies. Mr. Rauch has visited The Vitamin Shoppe website frequently, and has done so as recently as a few months ago. The TikTok SDK was installed on The Vitamin Shoppe website. Thus, unbeknownst to Mr. Rauch, when he visited The Vitamin Shoppe website, Defendants stole his Private Data through

the TikTok SDK including what health supplements he searched for, browsed, and purchased.

136. Mr. Rauch has also from time to time browsed and viewed videos on the website of nonprofit organization Feeding America in order to find opportunities for volunteer work. Mr. Rauch was able to do so without reviewing Feeding America's privacy policy. Mr. Rauch has visited Feeding America frequently, and has done so as recently as six months ago. The TikTok SDK was installed on Feeding America's website. Thus, unbeknownst to Mr. Rauch, when he visited Feeding America's website, Defendants stole his Private Data through the TikTok SDK, including what volunteer opportunities he considered.

137. Mr. Rauch is very conscious about his online privacy. He is a user of the Microsoft Edge and Google Chrome browsers. On both browsers, Mr. Rauch has changed his settings to block third-party cookies and has enabled the "do not track" function. He also utilizes McAfee security software to protect his online privacy. Despite Mr. Rauch's efforts, the TikTok SDK circumvents these measures and obtains his Private Data, by among other things transmuting third-party cookie into a first-party cookie.

138. The value of Mr. Rauch's Private Data has been diminished due to the fact that Defendants make available extensive information about his consumer preferences and activity without compensating him in any way.

139. The Rite Aid, Vitamin Shoppe, and Feeding America websites are just some representative examples of non-TikTok websites where Defendants have stolen the Private Data of Mr. Rauch and Class and Subclass members. Upon information and belief, the TikTok SDK is installed on at least 500,000 non-TikTok websites, including many popular websites visited on a day-to-day basis by millions of Americans including Mr. Rauch and Class and Subclass members.

E. Jacob Watters

140. Plaintiff Jacob Watters is a resident of Madison County, Illinois. Mr. Watters has never been a registered user of the TikTok app or held any TikTok account. He made a conscious decision not to do so because, like many other Americans, he was concerned that TikTok would violate his privacy.

141. Unbeknownst to Mr. Watters, several of the non-TikTok websites that he frequently visited have installed the TikTok SDK. Defendants secretly intercepted and collected his Private Data from these websites through the TikTok SDK, including browsing history and search queries. This is precisely what Mr. Watters wanted to avoid when he chose not to become a registered user of the TikTok app or hold any TikTok account.

142. For example, for at least the past two years, Mr. Watters has been a member of Upwork, a website that connects freelancers with job offers. Since then, Mr. Watters has on several occasions browsed and searched for various services and job offers on Upwork, as well as viewed videos. Mr. Watters last visited Upwork within the past year. Mr. Watters was able to sign up for an account with Upwork, and search for and browse job offers and services, and view videos without reviewing Upwork's privacy policies. The TikTok SDK was and is installed on Upwork. Thus, unbeknownst to Mr. Watters, when he visited Upwork, Defendants stole his Private Data through the TikTok SDK. This includes information on what services and job offers he searched or browsed for, and what videos he viewed.

143. Mr. Watters is very conscious about his online privacy. He is a user of the Google Chrome and Mozilla Firefox browsers. On both browsers, Mr. Watters has changed his settings to block third-party cookies and has enabled the "do not track" function. Despite Mr. Watters' efforts, the TikTok SDK circumvents these measures and obtains his Private Data, by among other things transmuting third-party cookie into a first-party cookie.

144. Mr. Watters has previously signed up to several consumer surveys, but has not yet been selected to participate. The value of Mr. Watters' Private Data has been diminished due to the fact that Defendants make available extensive information about his consumer preferences and activity without compensating him in any way.

145. The Upwork website is just one representative example of non-TikTok websites where Defendants have stolen the Private Data of Mr. Watters and Class and Subclass members. Upon information and belief, the TikTok SDK is installed on at least 500,000 non-TikTok websites, including many popular websites visited on a day-to-day basis by millions of Americans including Mr. Watters and Class and Subclass members.

VII. CLASS ALLEGATIONS

146. Plaintiffs incorporate by reference all foregoing allegations.

147. Pursuant to Federal Rule of Civil Procedure 23 ("Rule 23"), Plaintiffs seek to represent the following classes:

The First Nationwide Class: All natural persons residing in the United States who visited a website with the TikTok SDK software installed during the Class Period, and who have never been registered users of the TikTok app or held any TikTok account.

The First California Subclass: All natural persons residing in the state of California who visited a website with the TikTok SDK software installed during the Class Period, and who have never been registered users of the TikTok app or held any TikTok account.

The Nationwide Cookie Blocking Class: All natural persons residing in the United States who visited a website with the TikTok SDK software installed during the Class Period, who have never been registered users of the TikTok app or held any TikTok account, and who had web browser or system settings turned on to block third-party cookies.

The California Cookie Blocking Subclass: All natural persons residing in the state of California who visited a website with the TikTok SDK software installed during the Class Period, who have never been registered users of the TikTok app or held any TikTok account, and who had web browser or system settings turned on to block third-party cookies.

The Nationwide ECPA Class: All natural persons residing in the United States who have never been registered users of the TikTok app or held any TikTok account, and who visited a website that, during the Class Period, had the TikTok Pixel software installed but without "Search" as an optional event from the TikTok Pixel configuration menu**.**

The California ECPA Subclass: All natural persons residing in the State of California who have never been registered users of the TikTok app or held any TikTok account, and who visited a website that, during the Class Period, had the TikTok Pixel software installed but without "Search" as an optional event from the TikTok Pixel configuration menu**.**

148. In the alternative, Plaintiffs seek to represent the following classes:

The Rite Aid Nationwide Class: All natural persons residing in the United States who visited the Rite Aid website during the Class Period, and who have never been registered users of the TikTok app or held any TikTok account.

The Rite Aid California Subclass: All natural persons residing in the state of California who visited the Rite Aid website during the Class Period, and who have never been registered users of the TikTok app or held any TikTok account.

The Hulu Nationwide Class: All natural persons residing in the United States who visited the Hulu website during the Class Period, and who have never been registered users of the TikTok app or held any TikTok

account.

The Hulu California Subclass: All natural persons residing in the state of California who visited the Hulu website during the Class Period, and who have never been registered users of the TikTok app or held any TikTok account.

The Etsy Nationwide Class: All natural persons residing in the United States who visited the Etsy website during the Class Period, and who have never been registered users of the TikTok app or held any TikTok account.

The Etsy California Subclass: All natural persons residing in the state of California who visited the Etsy website during the Class Period, and who have never been registered users of the TikTok app or held any TikTok account.

The Build-a-Bear Workshop Nationwide Class: All natural persons residing in the United States who visited the Build-a-Bear Workshop website during the Class Period, and who have never been registered users of the TikTok app or held any TikTok account.

The Build-a-Bear Workshop California Subclass: All natural persons residing in the state of California who visited the Build-a-Bear Workshop website during the Class Period, and who have never been registered users of the TikTok app or held any TikTok account.

The Upwork Nationwide Class: All natural persons residing in the United States who visited the Upwork website during the Class Period, and who have never been registered users of the TikTok app or held any TikTok account.

The Upwork California Subclass: All natural persons residing in the state of California who visited the Upwork website during the Class Period, and who have never been registered users of the TikTok app or

held any TikTok account.

The Vitamin Shoppe Nationwide Class: All natural persons residing in the United States who visited The Vitamin Shoppe website during the Class Period, and who have never been registered users of the TikTok app or held any TikTok account.

The Vitamin Shoppe California Subclass: All natural persons residing in the state of California who visited Vitamin Shoppe website during the Class Period, and who have never been registered users of the TikTok app or held any TikTok account.

The Feeding America Nationwide Class: All natural persons residing in the United States who visited The Feeding America website during the Class Period, and who have never been registered users of the TikTok app or held any TikTok account.

The Feeding America California Subclass: All natural persons residing in the state of California who visited the Feeding America website during the Class Period, and who have never been registered users of the TikTok app or held any TikTok account.

149. The Class Period begins on the date that Defendants first received Private Data from non-TikTok users of websites on which the TikTok SDK was and/or is installed, as a result of the TikTok SDK, and continues through the present.

150. Plaintiffs reserve the right to modify or refine the definitions of the First Nationwide Class, First California Subclass, Nationwide Cookie Blocking Class, California Cookie Blocking Subclass, Nationwide ECPA Class, California ECPA Subclass, Rite Aid Nationwide Class, Rite Aid California Subclass, Hulu Nationwide Class, Hulu California Subclass, Etsy Nationwide Class, Etsy California Subclass, Build-a-Bear Workshop Nationwide Class, and Build-a-Bear Workshop California Subclass, Upwork Nationwide Class, Upwork California Subclass, The Vitamin Shoppe Nationwide Class, The Vitamin Shoppe California Subclass, Feeding

America Nationwide Class, and Feeding America California Subclass based upon discovery of new information and to accommodate any of the Court's manageability concerns.

151. Excluded from the Classes and Subclasses are: (i) any judge or magistrate judge presiding over this action and members of their staff, as well as members of their families; (ii) Defendants, Defendants' predecessors, parents, successors, heirs, assigns, subsidiaries, and any entity in which any Defendant or its parents have a controlling interest, as well as Defendants' current or former employees, agents, officers, and directors; (iii) persons who properly execute and file a timely request for exclusion from the class; (iv) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (v) counsel for Plaintiffs and Defendants; and (vi) the legal representatives, successors, and assigns of any such excluded persons.

152. **Numerosity (Rule 23(a)(1)).** The Classes and Subclasses are so numerous that joinder of individual members therein is impracticable. The exact number of Class and Subclass members, as herein identified and described, is not known, but each of the websites cited as illustrative examples in this Complaint are known to have millions of users based on publicly available data.

153. **Commonality (Rule 23(a)(2))**. Common questions of fact and law exist for each cause of action and predominate over questions affecting only individual Class and Subclass members, including the following:

(a) Whether Defendants used the TikTok SDK to read, attempt to read, learn, attempt to learn, eavesdrop, record, use, intercept, receive, and/or collect electronic communications of Private Data from Plaintiffs and Class and Subclass members during the Class Period;

(b) Whether Defendants' practice of using the TikTok SDK to read, attempt to read, learn, attempt to learn, eavesdrop, record, and/or use electronic communications of Private Data from Plaintiffs and Class and Subclass

members during the Class Period, violates the California Invasion of Privacy Act, Cal. Pen. Code § 630 *et seq.*;

(c) Whether Defendants' practice of intercepting, receiving, and/or collecting electronic communications of Private Data from Plaintiffs and Class and Subclass members through the TikTok SDK violates the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq.*;

(d) Whether Defendants' practice of intercepting, receiving, and/or collecting electronic communications of Private Data from Plaintiffs and Class and Subclass members through the TikTok SDK violates Cal. Pen. Code §§ 484, 496;

(e) Whether Defendants' practice of intercepting, receiving, and/or collecting electronic communications of Private Data from Plaintiffs and Class and Subclass members through the TikTok SDK constitutes conversion under California law;

(f) Whether Defendants' practice of intercepting, receiving, and/or collecting electronic communications of Private Data from Plaintiffs and Class and Subclass members through the TikTok SDK violates the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq.*;

(g) Whether Defendants' practice of intercepting, receiving, and/or collecting electronic communications of Private Data from Plaintiffs and Class and Subclass members through the TikTok SDK violates the California Constitution and/or qualifies as an intrusion upon seclusion under California law;

(h) Whether Defendants' practice of using the TikTok SDK to intercept, disclose, or intentionally use electronic communications of Private Data from Plaintiffs and Class and Subclass members during the Class

Period, violates the Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq.*;

(i) Whether profits obtained by Defendants through the use of Private Data that they obtained from Plaintiffs and Class and Subclass members were unjustly obtained and should be disgorged;

(j) Whether Defendants sold Private Data or access to Private Data unlawfully obtained from Plaintiffs and Class and Subclass members through the TikTok SDK;

(k) Whether Plaintiffs and Class and Subclass members sustained damages as a result of Defendants' alleged conduct, and, if so, what is the appropriate measure of damages and/or restitution; and

(l) Whether Plaintiffs and Class and Subclass members are entitled to declaratory and/or injunctive relief to enjoin the unlawful conduct alleged herein.

154. **Typicality (Rule 23(a)(3))**. Plaintiffs' claims are typical of the claims of members of the Classes and Subclasses because, among other things, Plaintiffs and members of the Classes and Subclasses sustained similar injuries as a result of Defendants' uniform wrongful conduct and their legal claims all arise from the same events and wrongful conduct by Defendants.

155. **Adequacy (Rule 23(a)(4)):** Plaintiffs will fairly and adequately protect the interests of the Classes and Subclasses. Plaintiffs' interests do not conflict with the interests of the Classes and Subclasses, and Plaintiffs have retained counsel with experience in complex class actions, as well as sufficient financial and legal resources to prosecute this case on behalf of the Classes and Subclasses. Plaintiffs and their counsel have no interest that is in conflict with, or otherwise antagonistic to the interests of the other Class and Subclass members. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the members of the

Classes and Subclasses. Plaintiffs anticipate no difficulty in the management of this litigation as a class action.

156. **Predominance & Superiority (Rule 23(b)(3)):** In addition to satisfying the prerequisites of Rule 23(a), Plaintiffs satisfy the requirements for maintaining a class action under Rule 23(b)(3). Common questions of law and fact predominate over any questions affecting only individual members of the Classes and Subclasses, and a class action is superior to individual litigation and all other available methods for the fair and efficient adjudication of this controversy. Here, common issues predominate because liability can be determined on a class-wide basis, even where some individualized damages determination may be required. Individualized litigation also presents a potential for inconsistent or contradictory judgments, and increases the delay and expense presented by complex legal and factual issues of the case to all parties and the court system. Furthermore, the expense and burden of individual litigation make it impossible for Class and Subclass members to individually redress the wrongs done to them. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

VIII. CALIFORNIA LAW APPLIES TO ALL THE CLASSES AND SUBCLASSES

157. California substantive law applies to Plaintiffs and every member of the Classes and Subclasses. California substantive law may be constitutionally applied to the claims of Plaintiffs and Class and Subclass members under the Due Process Clause, 14th Amend. § 1, and the Full Faith and Credit Clause, Art. IV. § 1 of the U.S. Constitution. California has significant contacts, or significant aggregation of contacts, to the claims asserted by Plaintiffs and Class and Subclass members, thereby creating state interests to ensure that the choice of California state law is not arbitrary or unfair.

158. Defendants' principal place of business is in California and Defendant TikTok, Inc. is a California corporation. Given Defendants' substantial business in California, California has an interest in regulating their conduct under its laws. Given Defendants' decision to avail themselves of California's laws, the application of California law to the claims herein is constitutionally permissible.

159. Further, three Plaintiffs and a substantial number of Class and Subclass members are located in California.

160. The application of California law to all proposed class and subclass members (defined above) is also appropriate under California's choice of law rules, namely, the governmental interest test California uses for choice-of-law questions. California's interest would be the most impaired if its laws were not applied.

IX. CAUSES OF ACTION

FIRST CAUSE OF ACTION

(Violation of the California Invasion of Privacy Act, Cal. Pen. Code § 630 *et seq.* – By Plaintiffs, the Classes, and the Subclasses Against All Defendants)

161. Plaintiffs, individually and on behalf of the Classes and Subclasses, incorporate the foregoing allegations as if fully set forth herein.

162. The California Invasion of Privacy Act ("CIPA"), codified at Cal. Pen. Code §§ 630-638, begins by providing its statement of purpose:

> The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

Cal. Pen. Code § 630.

163. Cal. Pen. Code § 631(a) imposes liability upon:

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner . . . willfully and ***without the consent of all parties*** to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over

> any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to lawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section . . . . [Emphasis added.]

164. Cal. Pen. Code § 632(a) imposes liability upon:

> A person who, intentionally and ***without the consent of all parties*** to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio [Emphasis added.]

165. Under either section of the CIPA quoted above, a defendant must show it had the consent of all parties to a communication.

166. Defendants knowingly and intentionally used and continue to use the TikTok SDK and receiving servers (where the Private Data was and is saved and recorded), both of which are recording devices under CIPA, to read, attempt to read, learn, attempt to learn, eavesdrop, record, and/or use electronic communications containing Private Data from Plaintiffs and Class and Subclass members, while these electronic communications were and are in transit, originating in or sent to California, and without the authorization or consent of Plaintiffs, Class members, or Subclass members.

167. Plaintiffs and Subclass members were and are in California during one or more of the instances where Defendants intercepted their communications. Upon information and belief, each Class and Subclass member, even those located outside of California, during one or more of their interactions on the Internet during the applicable statute of limitations period, communicated with one or more entities based in California, and/or with one or more entities whose servers were located in California. Communications from the California web-based entities to Class and Subclass members were sent from California. Communications to the California web-based entities from Class and Subclass members were sent to California.

168. The communications intercepted by Defendants include "contents" of electronic communications exchanged between Plaintiffs and Class and Subclass members, on the one hand, and the websites where the TikTok SDK was installed, on the other, in the form of detailed URL requests, webpage browsing histories and search queries, and URLs containing the specific search queries. Defendants' non-consensual interception of these communications was designed to learn at least some of these contents.

169. The following items constitute "machine[s], instrument[s], or contrivance[s]" under Cal. Penal Code § 631(a), and even if they did not, Defendants' purposeful scheme that facilitated its interceptions falls under the broad statutory catch-all category of "any other manner":

(a) Plaintiffs' and Class and Subclass members' browsers;

(b) Plaintiffs' and Class and Subclass members' personal computing devices;

(c) the computer codes and programs used by Defendants to effectuate the interception of communications exchanged between websites and search engines, on the one hand, and Plaintiffs and Class and Subclass members, on the other;

(d) Defendants' servers, at least some of which, on information and belief, are located in California;

(e) the servers of the non-TikTok websites from which Defendants' intercepted Plaintiffs' and Class and Subclass members' communications;

(f) the plan Defendants carried out to effectuate the interception of the communications that were exchanged between the non-TikTok websites, on the one hand, and Plaintiffs and Class and Subclass members, on the other.

170. The Private Data collected by Defendants constituted "confidential communications," as that term is used in Cal. Pen. Code § 632(a), because Plaintiffs and Class and Subclass members have an objectively reasonable expectation of privacy that their private browsing communications are not being intercepted, collected, or disseminated by Defendants—particularly given that Plaintiffs and Class and Subclass members had never been registered users of the TikTok app or held any TikTok accounts.

171. Plaintiffs and Class and Subclass members have suffered loss because of these violations, including, but not limited to, violation of their rights to privacy and loss of value in their Private Data.

172. Pursuant to Cal. Pen. Code § 637.2, Plaintiffs and Class and Subclass members have been injured by the violations of Cal. Pen. Code §§ 631, 632, and each seeks damages for the greater of $5,000 or three times the amount of actual damages, as well as injunctive or other equitable relief.

SECOND CAUSE OF ACTION

(Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq.* – By Plaintiffs, the Classes, and the Subclasses Against All Defendants)

173. Plaintiffs, individually and on behalf of the Classes and Subclasses, incorporate the foregoing allegations as if fully set forth herein.

174. Plaintiffs' and Class and Subclass members' devices used to access the non-TikTok websites are, and at all relevant times have been, used for interstate communication and commerce, and are therefore "protected computers" under 18 U.S.C. § 1030I(2)(B). Plaintiffs' and Class and Subclass members' Internet browsing, which Defendants impermissibly tracked, involved submissions to websites for companies all over the United States, both for purchases of goods and information.

175. Defendants have exceeded, and continue to exceed, authorized access to Plaintiffs' and Class and Subclass members' protected computers and obtained information from them, in violation of 18 U.S.C. § 1030(a)(2).

176. Defendants' conduct also constitutes "a threat to public health or safety" under 18 U.S.C. § 1030(c)(4)(A)(i)(IV), due to the private and personally identifiable data and content of Plaintiffs and Class and Subclass members being made available to foreign actors, potentially including foreign intelligence services, in locations without adequate legal privacy protections. The fact that this threat is real and imminent is evidenced by, among other facts discussed in detail above, the U.S. Senate's ongoing scrutiny on TikTok's collection and storage of data on ordinary Americans, TikTok's ties to and control by its Chinese parent company, Montana's ban on the use of the TikTok app, and proposed federal legislation that would entirely ban or significant curtail the domestic use of the TikTok app.

177. Accordingly, Plaintiffs and Class and Subclass members are entitled to "maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g).

THIRD CAUSE OF ACTION

(Statutory Larceny, Cal. Pen. Code §§ 484, 496 – By Plaintiffs, the Classes, and the Subclasses Against All Defendants)

178. Plaintiffs, individually and on behalf of the Classes and Subclasses, incorporate the foregoing allegations as if fully set forth herein.

179. Cal. Pen. Code § 496 imposes liability upon:

> [e]very person who buys or receives any property that has been stolen or that has been obtained in any manner constituting theft or extortion, knowing the property to be so stolen or obtained, or who conceals, sells, withholds, or aids in concealing, selling, or withholding any property from the owner, knowing the property to be so stolen or obtained[.]

180. Cal. Pen. Code § 484, which defines "theft", states in pertinent part:

> Every person who shall feloniously steal, take, carry, lead, or drive away the personal property of another, or who shall fraudulently appropriate property which has been entrusted to him or her, or who shall knowingly

> and designedly, by any false or fraudulent representation or pretense, defraud any other person of money, labor or real or personal property, or who causes or procures others to report falsely of his or her wealth or mercantile character and by thus imposing upon any person, obtains credit and thereby fraudulently gets or obtains possession of money, or property or obtains the labor or service of another, is guilty of theft.

181. Under California law, Plaintiffs' and Class and Subclass members' Private Data constitutes property that can be the subject of theft.

182. Defendants acted in a manner constituting theft by surreptitiously taking Plaintiffs' and Class and Subclass members' Private Data through the TikTok SDK installed on non-TikTok websites, with the specific intent to deprive Plaintiffs and Class and Subclass members of their property.

183. Plaintiffs and Class and Subclass members did not consent to any of Defendants' actions in taking Plaintiffs' and Class and Subclass members' Private Data.

184. Pursuant to Cal. Pen. Code § 496(c), Plaintiffs and Class and Subclass members are entitled to treble damages, as well as attorneys' fees and costs, for injuries sustained as a result of Defendants' violations of Cal. Pen. Code § 496(a).

FOURTH CAUSE OF ACTION

(Conversion – By Plaintiffs, the Classes, and the Subclasses Against All Defendants)

185. Plaintiffs, individually and on behalf of the Classes and Subclasses, incorporate the foregoing allegations as if fully set forth herein.

186. Property is the right of any person to possess, use, enjoy, or dispose of a thing, including intangible things such as data or communications. Plaintiffs' and Class and Subclass members' Private Data is their property under California law.

187. Defendants unlawfully intercepted, collected, used, and exercised dominion and control over Plaintiffs' and Class and Subclass members' Private Data without authorization.

188. Defendants wrongfully exercised control over Plaintiffs' and Class and Subclass members' Private Data, and have not returned such Private Data.

189. Plaintiffs and Class and Subclass members have been damaged as a result of Defendants' unlawful conversion of their property.

FIFTH CAUSE OF ACTION

(Violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq.* – By Plaintiffs, the Classes, and the Subclasses Against All Defendants)

190. Plaintiffs, individually and on behalf of the Classes and Subclasses, incorporate the foregoing allegations as if fully set forth herein.

191. California's Unfair Competition Law ("UCL") prohibits any "unlawful, unfair, or fraudulent business act or practice." Cal. Bus. & Prof. Code §17200.

192. Defendants engaged in "unlawful" conduct through their violation of state and federal law, including (a) violation of the California Invasion of Privacy Act, Cal. Pen. Code § 630 *et seq*.; (b) violation of the Computer Fraud and Abuse Act**,** 18 U.S.C. § 1030 *et seq*.; (c) violation of Cal. Pen. Code §§ 484, 496; (d) conversion; (e) invasion of privacy under Article I, Section 1 of the California Constitution; and (f) intrusion upon seclusion.

193. Defendants engaged in "unfair" conduct, because they knowingly intercepted and collected communications, and/or knowingly received intercepted communications, containing the Private Data of Plaintiffs and Class and Subclass members under circumstances in which Plaintiffs and Class and Subclass members would have no reason to know that such information was being intercepted because it was never disclosed or otherwise made known to them by Defendants.

194. Plaintiffs and Class and Subclass members have suffered injury-in-fact, including the loss of money and/or property as a result of Defendants' unfair and/or unlawful practices, to wit, the unauthorized collection of their Private Data, which has value in an amount to be proven at trial. Moreover, Plaintiffs and Class and

Subclass members have suffered harm in the form of diminution of the value of their Private Data.

195. Defendants' actions caused damage to and loss of Plaintiffs' and Class and Subclass members' property right to control the dissemination and use of their Private Data.

196. Defendants have taken property from Plaintiffs and Class and Subclass members without providing just, or any, compensation.

197. Defendants should be required to cease their unfair and/or illegal collection of user data and to retrieve and delete all unfairly and/or illegally obtained user data. Defendants reaped unjust profits and revenues in violation of the UCL. Plaintiffs and Class and Subclass members seek injunctive relief governing Defendants' ongoing taking and possession of their Private Data, and/or failure to account to Plaintiffs and Class and Subclass members concerning Defendants' interception, collection, possession, and use of Plaintiffs' and Class and Subclass members' Private Data, and restitution and disgorgement of resulting unjust profits and revenues to Defendants.

198. Plaintiffs and Class and Subclass members lack an adequate remedy at law because the ongoing harms from Defendants' interception, collection, taking, possession, and use of Private Data must be addressed by injunctive relief and, due to the ongoing and nature of the harm, the harm cannot be adequately addressed by monetary damages alone.

SIXTH CAUSE OF ACTION

(Invasion of Privacy under Article I, Section 1 of the California Constitution – By Plaintiffs, the Classes, and the Subclasses Against All Defendants)

199. Plaintiffs, individually and on behalf of the Classes and Subclasses, incorporate the foregoing allegations as if fully set forth herein.

200. In 1972, California added a right of privacy to the list of enumerated inalienable rights in Article I, Section 1 of its Constitution.

201. The right to privacy was added to the California Constitution after voters approved a legislative constitutional amendment designated as Proposition 11. Critically, the argument in favor of Proposition 11 reveals that the legislative intent was to curb businesses' control over the unauthorized collection and use of consumers' personal information, stating:

> The right to privacy is the right to be left alone . . . It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. Fundamental to our privacy is the ability to control circulating of personal information. This is essential to social relationships and personal freedom.[80]

202. The principal purpose of this Constitutional right was to protect against unnecessary information gathering, use, and dissemination by public and private entities, including Defendants.

203. The right to privacy in California's Constitution creates a right of action against private entities like the Defendants.

204. To plead invasion of privacy under the California Constitution, Plaintiffs and Class and Subclass members must allege "that (1) they possess a legally protected privacy interest, (2) they maintain a reasonable expectation of privacy, and (3) the intrusion is 'so serious . . . as to constitute an egregious breach of the social norms' such that the breach is 'highly offensive.'" *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 601 (9th Cir. 2020), quoting *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 287 (2009).

205. Plaintiffs and Class and Subclass members have a legally protected privacy interest in (a) precluding the interception, collection, copying, dissemination and/or misuse of their Private Data; and (b) making personal decisions and/or conducting personal activities without observation, intrusion or interference, including, but not limited to, the right to visit and interact with various internet sites

[80] BALLOT PAMP., PROPOSED STATS. & AMENDS. TO CAL. CONST. WITH ARGUMENTS TO VOTERS, GEN. ELECTION *26 (NOV. 7, 1972).

without having that information intercepted and transmitted to Defendants without Plaintiffs' and Class and Subclass members' knowledge or consent.

206. Plaintiffs and Class and Subclass members have a reasonable expectation of privacy in the Private Data that Defendants intercept and collect without adequate notice or consent—particularly given that Plaintiffs and Class and Subclass members had never been registered users of the TikTok app or held any TikTok accounts.

207. Defendants' actions constitute a serious invasion of privacy in that they: (a) invade a zone of privacy protected by the Fourth Amendment, namely, the right to privacy in data contained on personal computing devices, including web search and browsing histories; (b) violate federal criminal laws including the Computer Fraud and Abuse Act; and (c) invade the privacy interests and rights of millions of U.S. residents (including Plaintiffs and Class and Subclass members) without their consent.

208. Defendants' surreptitious and unauthorized interception and collection—through the TikTok SDK installed on non-TikTok websites—of the internet communications of millions of U.S. residents who have made the conscious decision not to interact with Defendants or the TikTok app constitutes an egregious breach of social norms that is highly offensive. This behavior is doubly offensive because the Private Data intercepted and collected is paired with other secretly collected data, such as data collected from multiple websites installed with the TikTok SDK, resulting in Defendants creating digital dossiers of individuals. This conduct is even more offensive where Defendants evade the browser or system settings in place to block third-party tracking.

209. Defendants lacked a legitimate business interest in intercepting and receiving private internet communications between Plaintiffs and Class and Subclass members, on the one hand, and the non-TikTok websites with the TikTok SDK

installed, on the other, without first obtaining the consent of Plaintiffs and Class and Subclass members.

210. Plaintiffs and Class and Subclass members have sustained, and will continue to sustain, damages as a direct and proximate result of Defendants' invasion of their privacy and are entitled to just compensation and injunctive relief, as well as such other relief as the Court may deem just and proper.

SEVENTH CAUSE OF ACTION

(Intrusion Upon Seclusion – By Plaintiffs, the Classes, and the Subclasses Against All Defendants)

211. Plaintiffs, individually and on behalf of the Classes and Subclasses, incorporate the foregoing allegations as if fully set forth herein.

212. A claim for intrusion upon seclusion requires (1) intrusion into a private place, conversation, or matter; (2) in a manner highly offensive to a reasonable person.

213. By intercepting the internet communications of Plaintiffs and Class and Subclass members, on one hand, and non-TikTok websites with the TikTok SDK installed, on the other, Defendants intentionally intruded upon the solitude and/or seclusion of Plaintiffs and Class and Subclass members.

214. Defendants' intrusion was intentional. Defendants intentionally designed the TikTok SDK and underlying programming code to surreptitiously intercept, collect, and retain the Private Data of Plaintiffs and Class and Subclass members. Defendants effectively place themselves in the middle of conversations. Defendants also intentionally intruded upon Plaintiffs' and Class and Subclass members' solitude, seclusion, and private affairs by intentionally receiving and using this Private Data for their own benefit, knowing how it had been obtained.

215. Defendants intercept these internet communications containing Private Data without authority or consent from Plaintiffs and Class and Subclass members.

216. Defendants' intentional intrusion into Plaintiffs' and Class and Subclass members' internet communications, computing devices, and web browsers is highly offensive to a reasonable person in that such intrusions violate federal and state criminal and civil laws designed to protect individual privacy and guard against theft. Such behavior is doubly offensive because the Private Data intercepted and collected is paired with other secretly collected data from other websites with the TikTok SDK installed, allowing Defendants to create unique digital dossiers. This conduct is even more offensive where Defendants evade the browser or system settings in place to block third-party tracking.

217. Plaintiffs and Class and Subclass members reasonably expected that their Private Data would not be intercepted, collected, stored, or used by Defendants, particularly given that Plaintiffs and Class and Subclass members had never been registered users of the TikTok app or held any TikTok accounts.

218. Plaintiffs and Class and Subclass members have sustained, and will continue to sustain, damages as a direct and proximate result of Defendants' intrusions and are entitled to just compensation and injunctive relief, as well as such other relief as the Court may deem just and proper.

219. Plaintiffs and Class and Subclass members have been damaged by these intrusions, which have allowed Defendants to obtain profits that rightfully belong to Plaintiffs and Class and Subclass members. Plaintiffs and Class and Subclass members are entitled to reasonable compensation including but not limited to disgorgement of profits related to the unlawful intrusion into their private internet communications.

EIGHTH CAUSE OF ACTION

(Violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq.* – By Plaintiffs, the Classes, and the Subclasses Against All Defendants)

220. Plaintiffs, individually and on behalf of the Classes and Subclasses, incorporate the foregoing allegations as if fully set forth herein.

221. The Federal Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986 ("ECPA"), proscribes the intentional interception, disclosure, or use of the contents of any wire, oral, or electronic communication through the use of a device. 18 U.S.C. § 2511.

222. The statute provides a private right of action to "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter." 18 U.S.C. § 2520(a).

223. The Federal Wiretap Act protects both the sending and receipt of electronic communications.

224. Plaintiffs and Class and Subclass members, as individuals, are persons within the meaning of 18 U.S.C. § 2510(6).

225. Defendants knowingly and intentionally used and continue to use the TikTok SDK and receiving servers (where the Private Data was and is saved and recorded), both of which are devices under ECPA, to intercept electronic communications containing Private Data from Plaintiffs and Class and Subclass members, while these electronic communications were and are in transit, without the authorization or consent of Plaintiffs, Class members, or Subclass members. Defendants are sophisticated software companies that know the TikTok SDK is intercepting communications in these circumstances and have taken no remedial action.

226. ECPA defines "contents" as including "any information concerning the substance, purport, or meaning of [a] communication." 18 U.S.C. § 2510(8). The communications intercepted by Defendants include "contents" of electronic communications exchanged between Plaintiffs and Class and Subclass members, on the one hand, and the non-TikTok websites where the TikTok SDK was installed, on the other, in the form of detailed URL requests, webpage browsing histories and search queries, and URLs containing the specific search queries. Defendants' non-

consensual interception of these communications was designed to learn at least some of these contents.

227. The transmission of data between Plaintiffs and Class and Subclass members, on the one hand, and the non-TikTok websites with which they chose to exchange communications, on the other, constitutes the "transfer[s] of signs, signals, writing, . . . data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce." The transmitted data is therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

228. The following constitute "devices" as defined under 18 U.S.C. § 2510(5) of the Act:

(a) Plaintiffs' and Class and Subclass members' browsers;

(b) Plaintiffs' and Class and Subclass members' personal computing devices;

(c) the computer codes and programs used by Defendants to effectuate the interception of communications exchanged between websites and search engines, on the one hand, and Plaintiffs and Class and Subclass members, on the other;

(d) Defendants' servers;

(e) the servers of the non-TikTok websites from which Defendants' intercepted Plaintiffs' and Class and Subclass members' communications;

(f) the plan Defendants carried out to effectuate the interception of the communications that were exchanged between the non-TikTok websites, on the one hand, and Plaintiffs and Class and Subclass members, on the other.

229. For purposes of this Complaint, Defendants are not "electronic communication service[s]," as defined in 18 U.S.C. § 2510(12), nor are they Internet Service Providers.

230. Defendants' unlawful interception of electronic communications is not excused under 18 U.S.C. § 2511(2)(c) because Defendants are not parties to the communication, have not received prior consent to engage in some interception from Plaintiffs or Class or Subclass members, and have in at least some instances not received prior consent from the non-TikTok websites visited by Plaintiffs and Class and Subclass members.

231. Specifically, as discussed in more detail *supra*, regardless of how a non-TikTok website configures the TikTok Pixel, it will always collect information on PageView events of website visitors as a nonnegotiable baseline. PageView events contain full-string URLs, which provide Defendants with the search terms of each user. However, Defendants do not disclose to these non-TikTok websites that the PageView event encompasses search terms.

232. Further, Defendants included "Search" as an ***optional*** event in the TikTok Pixel configuration menu. A reasonable individual would see that "Search" was an optional event and conclude that if they did not select "Search," no search terms would be collected. Defendants never disclosed that, regardless of whether or not a non-TikTok website selected the "Search" event, all search terms would be intercepted and collected through the default, nonnegotiable "PageView" event.

233. Thus, these non-TikTok websites that did not select "Search" as an optional event from the TikTok Pixel configuration menu never consented to Defendants' interception and collection of search terms. Defendants never disclosed that this information would be intercepted and collected, never gave the non-TikTok websites an option to "opt-out" of the collection by re-configuring the TikTok Pixel, and lulled the non-TikTok website operators into a false sense of security by presenting "Search" as an optional event.

234. Plaintiffs and Class and Subclass members have suffered loss because of these violations, including, but not limited to, violation of their rights to privacy and loss of value in their Private Data.

235. For the violations set forth above and pursuant to 18 U.S.C. § 2520, Plaintiffs and Class and Subclass members seek (1) appropriate preliminary and other equitable or declaratory relief; (2) damages, in an amount to be determined at trial, assessed as the greater of (a) the sum of the actual damages suffered by Plaintiffs and Class and Subclass members and any profits made by Defendants as a result of the violation, or (b) statutory damages of whichever is the greater of $100 per day per violation or $10,000; (3) punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by Defendants in the future; and (4) reasonable attorney's fees and other litigation costs reasonably incurred.

NINTH CAUSE OF ACTION

(Unjust Enrichment – By Plaintiffs, the Classes, and the Subclasses Against All Defendants)

236. Plaintiffs, individually and on behalf of the Classes and Subclasses, incorporate the foregoing allegations as if fully set forth herein.

237. Plaintiffs and Class and Subclass members conferred a benefit on Defendants in the form of Private Data which has substantial monetary value that Defendants extracted and used to produce revenue and unjustly retained those benefits at the expense of Plaintiffs and Class and Subclass members.

238. Defendants intercepted, collected, and used and made available this information for their own gain, reaping economic, intangible, and other benefits.

239. Defendants unjustly retained those benefits at the expense of Plaintiffs and Class and Subclass members because Defendants' conduct damaged Plaintiffs and Class and Subclass members, all without providing any commensurate compensation to Plaintiffs and Class and Subclass members.

240. Plaintiffs and Class and Subclass members did not consent to the interception, collection, and use of their Private Data, nor did they have any control over its use. Therefore, under principles of equity and good conscience, Defendants should not be permitted to retain any money derived from their use of Plaintiffs and Class and Subclass members' Private Data.

241. The benefits that Defendants derived from Plaintiffs and Class and Subclass members rightly belong to Plaintiffs and Class and Subclass members. It would be inequitable under unjust enrichment principles to permit Defendants' retention of any of the profit or other benefits they derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

X. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs request relief against Defendants as set forth below:

a. Certifying the proposed Classes and Subclasses as requested herein pursuant to Federal Rule of Civil Procedure 23;

b. Entering an order appointing Plaintiffs as representatives of the Classes and Subclasses;

c. Entering an order appointing undersigned counsel to represent the Classes and Subclasses;

d. Entering Judgment in favor of each Class and Subclass member for damages suffered as a result of the conduct alleged herein, as well as punitive damages, restitution, disgorgement, the greater of $5,000 or three times the amount of actual damages pursuant to Cal. Pen. Code § 637.2, any profits made by Defendants as a result of the violation and the greater of $100 per day per violation or $10,000 pursuant to 18 U.S.C. § 2520, and treble damages pursuant to Cal. Pen. Code § 496, including interest and prejudgment interest;

e. Entering an order granting injunctive relief as permitted by law or equity, including enjoining Defendants from continuing any unlawful

practices as set forth herein, and directing Defendants to identify, with Court supervision, victims of their conduct and pay them all the money they are required to pay;

f. Awarding Plaintiffs and Class and Subclass members their reasonable costs and expenses incurred in this action, including attorneys' fees and costs;

g. Ordering that Defendants delete the Private Data that they intercepted and collected from Plaintiffs and Class and Subclass members; and

h. Providing any such further relief as the Court deems just and proper.

XI. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all issues so triable.

DATED: October 20, 2023

Ekwan E. Rhow
Marc E. Masters
Christopher J. Lee
BIRD, MARELLA, BOXER, WOLPERT, NESSIM, DROOKS, LINCENBERG & RHOW, P.C.

By: /s/ Ekwan E. Rhow
Ekwan E. Rhow
Attorneys for Plaintiffs Bernadine Griffith, Patricia Shih, Rhonda Irvin, Matthew Rauch, and Jacob Watters

DATED: October 20, 2023

Jonathan M. Rotter
Kara M. Wolke
Gregory B. Linkh
GLANCY PRONGAY & MURRAY LLP

By: /s/ Jonathan M. Rotter
Jonathan M. Rotter
Attorneys for Plaintiffs Bernadine Griffith, Patricia Shih, Rhonda Irvin, Matthew Rauch, and Jacob Watters

DATED: October 20, 2023

Kalpana Srinivasan
Steven Sklaver
Michael Gervais
Gloria Park
SUSMAN GODFREY L.L.P.

By: /s/ Michael Gervais
Michael Gervais
Attorneys for Plaintiffs Bernadine Griffith, Patricia Shih, Rhonda Irvin, Matthew Rauch, and Jacob Watters

ATTESTATION

Pursuant to L.R. 5-4.3.4, the filer attests that all signatories listed, and on whose behalf this filing is submitted, concur in its content and have authorized the filing.

DATED: October 20, 2023

Ekwan E. Rhow
Marc E. Masters
Christopher J. Lee
Bird, Marella, Boxer, Wolpert, Nessim, Drooks, Lincenberg & Rhow, P.C.

By: 

Ekwan E. Rhow
Attorneys for Plaintiffs Bernadine Griffith, Patricia Shih, Rhonda Irvin, Matthew Rauch, and Jacob Watters